Biometric Identification Standards Research

Final Report Volume I

James L. Wayman
Biometric Identification Research Director
College of Engineering
San Jose State University

December, 1997

Prepared under FWHA CONTRACT DTFH61-95-C-00165

BIOMETRIC IDENTIFICATION STANDARDS RESEARCH

FINAL REPORT
VOLUME I

James L. Wayman
Biometric Identification Research Director
College of Engineering
San Jose State University

December, 1997

Prepared under **FHWA CONTRACT DTFH61-95-C-00165**

ACKNOWLEDGEMENTS

Many people contributed greatly to this project and the creation of this report. Included text was written by Professors Jan Botha and Ken Nuger of San Jose State University. Phil Forjan, as the Contracting Officer for the Federal Highway Administration, was very active in the guidance and review of this project, as were Brian McLaughlin and Bob Redmond, also of FHWA. Sheila Prior of the American Association of Motor Vehicle Administrators organized the extensive review meetings of the Biometric Working Group, which were chaired by Gary Nishite of the California Department of Motor Vehicles. Gary Murata, also of the California Department of Motor Vehicles, was instrumental in the definition and organization of this effort. Philomena Blake of the San Jose State University Foundation handled the contract reporting details, and Dean Don Kirk and Associate Dean Nabil Ibrahim of the College of Engineering both supported and encouraged this project from the beginning. My sincerest thanks to all of you.

James L. Wayman
San Jose, California
October 1, 1997

FORWARD

When we began this project in October of 1995, there was no text book, no journal, and no general professional society in the area of biometric identification. It is not surprising, therefore, that there was no commonality in concepts, terminology, or testing and reporting methodologies. As of this writing, there is still no textbook, journal or professional society. However, there has been significant progress in the area of concepts, terminology and test and reporting methods. We believe that this project has made a strong and lasting contribution in these areas.

Much of our work on this project has already become canonical in the field: the taxonomy of applications discussed in Appendices A and B with the concepts of "cooperative" and "non-cooperative" applications; the systems diagram of Appendices C and D; the generalized terminology of "false match" and "false non-match" to replace the less precise, policy-dependent terms "false rejection/acceptance" and "Type I/II error"; the insistence that the reported "false match rate" be normalized by the number of comparisons made; the acknowledgement of Appendix F that "verification" is the degenerate case of "identification" and governed by the same system equations. Although the primary goal of this work has been to assist the Department of Transportation in complying with the requirements of Section 9105 of Public Law 100-690, a strong, secondary goal has been to create a framework for the future analysis of biometric systems by the federal government. It is our hope that this work will be judged by our success in meeting both of these objectives.

TABLE OF CONTENTS

0. EXECUTIVE SUMMARY **1**
0.1 INTRODUCTION 1
0.2 THE PURPOSE OF THE SYSTEM 1
0.3 WORK PLAN 1
0.4 TECHNOLOGY SELECTION 2
0.5 STANDARDS DEVELOPMENT 2
0.5.1 Finger Selection *3*
0.5.2 Image Quality *4*
0.5.3 Compression Method and Ratio *4*
0.5.4 Data Format Standard *5*
0.5.5 Minutiae Extraction *5*
0.6 THREE SYSTEM DESIGNS 5
0.6.1 The Centralized System *6*
0.6.2 The Distributed System with Centralized Communication *7*
0.6.3 The Distributed System with Direct Communication *8*
0.7 LEGAL CONSIDERATIONS 8
0.8 BENEFIT-COST ANALYSIS 9
0.9 CONCLUSIONS 10
1.0 THE HISTORY OF THE FHWA BIOMETRIC IDENTIFICATION STANDARDS PROJECT11
1.1 HOUSE SUBCOMMITTEE ON SURFACE TRANSPORTATION HEARINGS (1987) 11
1.2 THE TRUCK AND BUS SAFETY AND REGULATORY REFORM ACT OF 1988 12
1.3 THE MULTI-STATE STEERING COMMITTEE'S FUNCTIONAL REQUIREMENTS 13
1.4 THE ORKAND STUDIES 14
1.5 ADVANCED NOTICE OF PROPOSED RULE MAKING 1989 AND THE 24 QUESTIONS 14
1.6 PUBLIC RESPONSE 16
1.7 ADVANCED NOTICE OF PROPOSED RULEMAKING 1990 16
1.8 THE BROAD AGENCY ANNOUNCEMENT OF 1995 17
1.9 THE SAN JOSE STATE UNIVERSITY PROPOSAL 18
2.0 BIOMETRIC TECHNOLOGIES AND THE INTENT OF CONGRESS **18**
3.0 A PRIMER ON BIOMETRIC SYSTEMS **20**
3.1 THE DATA COLLECTION SUB-SYSTEM 21
3.2 THE TRANSMISSION SUB-SYSTEM 21
3.3 THE SIGNAL PROCESSING SUB-SYSTEM 21
3.4 THE STORAGE SUB-SYSTEM 23
3.5 THE DECISION SUB-SYSTEM 23
4.0 SYSTEM APPLICATIONS AND FUNCTIONS **23**
4.1 SYSTEM ALTERNATIVES 23
4.2 PREVENTION OF ISSUANCE OF MULTIPLE LICENSES 24
4.3 PREVENTION OF THE ISSUANCE OF GENUINE LICENSE TO FRAUDULENTLY IDENTIFIED DRIVER 26
4.4 DETECT THE USE OF FRAUDULENTLY OBTAINED LICENSE 27
4.5 DETECT THE USE OF MULTIPLE LICENSES BY A SINGLE DRIVER 29
5.0 A REVIEW OF THE MULTI-STATE STEERING COMMITTEE FUNCTIONAL REQUIREMENTS **29**
5.1 THE REVISED FUNCTIONAL REQUIREMENTS 30
5.2 AAMVA FUNCTIONAL REQUIREMENTS AND SYSTEM APPLICATIONS 32
6.0 CRITERIA FOR TECHNOLOGY SELECTION **32**
7.0 HOW CIVILIAN FINGERPRINTING SYSTEMS WORK **34**
7.1 THE DATA COLLECTION SUB-SYSTEM 34
7.2 THE TRANSMISSION SUB-SYSTEM 35
7.2.1 Signal Compression *35*
7.2.2 Data Transmission Format *37*
7.3 SIGNAL PROCESSING SUBSYSTEM 37
7.3.1 The Feature Extraction Module *37*

7.3.2 The Pattern Classification Module *38*
7.3.3 The Quality Control Module *40*
7.3.4 The Pattern Matcher *41*
7.4 STORAGE SUB-SYSTEM 42
7.4.1 Feature Storage *42*
7.4.2 Image Storage *42*
7.5 THE DECISION SUB-SYSTEM 42
7.6 FIELD VERIFICATION SYSTEMS 42
8.0 THE PROBLEMS WITH FINGERPRINTING 43
8.1 DECEPTIVE PRACTICES BY THE CUSTOMER 43
8.2 BAD PRINTS AND MISSING FINGERS 44
8.3 ADHERENCE TO STANDARDS 45
9. 0 PREDICTING AFIS PERFORMANCE IN APPLICATION TO COMMERCIAL DRIVERS. 45
9.1 SYSTEM PARAMETERS 45
9.2 PENETRATION RATE 46
9.3 BIN ERROR RATE 47
9.4 SINGLE COMPARISON FALSE MATCH RATE 47
9.5 SINGLE COMPARISON FALSE NON-MATCH RATE 48
9.6 SINGLE COMPARISON MATCH RATE AND SYSTEM THROUGHPUT 48
9.7 THE PHILIPPINE AFIS BENCHMARK TEST 49
9.7.1 Fingerprint Images *49*
9.7.2 Test Requirements *51*
9.7.3 AFIS Performance Results *51*
FIGURE 3 53
9.8 PERFORMANCE PREDICTION IN THE CDL ENVIRONMENT 54
10.0 A SURVEY ON THE USE OF FINGERPRINTING FOR DRIVER'S LICENSE APPLICATIONS 57
11.0 SYSTEMS ISSUES AND COMPETING ARCHITECTURES 58
11.1 A FEDERAL-LEVEL SYSTEM 58
11.2 A STATE-LEVEL SYSTEM 59
11.2.1 The Distributed System with Centralized Communication *59*
11.2.2 The Distributed System with Direct Communication *60*
12.0 LEGAL CONSIDERATIONS 61
12.1 SEARCH, SEIZURE AND SELF-INCRIMINATION CONSIDERATIONS 61
12.2 DUE PROCESS CONSIDERATIONS 63
12.3 STATE LAWS REGARDING INTER-STATE EXCHANGE OF BIOMETRIC INFORMATION 65
13.0 OUR RESPONSE TO THE 24 QUESTIONS OF THE ANPRM 66
14.0 FINGERPRINTING AND THE REVISED FUNCTIONAL REQUIREMENTS 70
15.0 STANDARDS DEVELOPMENT 73
15.1 A STANDARD BIOMETRIC IDENTIFIER 73
15.2 IMAGE QUALITY STANDARD 74
15.3 DATA COMPRESSION STANDARD 74
15.4 DATA FORMAT STANDARD 74
15.5 FEATURE SET STANDARD 74
16.0 BENEFIT-COST ANALYSIS 75
16.1 SOME PERTINENT ISSUES RELATED TO THE BENEFIT-COST ANALYSIS 76
16.1.1 Performance of Commercial Activities *76*
16.1.2 Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs *76*
16.1.3 Principles for Federal Infrastructure Investments *79*
16.1.4 Life-Cycle Cost Analysis *79*
16.1.5 Some Conclusions and Recommendations *80*
16.2 BENEFITS 80
16.3 SOME ESTIMATES OF BENEFITS 82
16.4 COSTS 84
16.5 REFERENCES FOR BENEFIT-COST STUDY 84
17.0 CONCLUSIONS 85

TABLE OF CONTENTS --VOLUME II

APPENDIX A: "Introduction to Biometrics: Towards a Science"
APPENDIX B: "The State of Biometrics"
APPENDIX C: "The Science of Biometric Technologies: Testing, Classifying, Evaluating"
APPENDIX D: "A Scientific Approach to Evaluating Biometric Systems Using a Mathematical Methodology"
APPENDIX E: "Large-Scale Civilian Identification Systems—Issues and Feasibility"
APPENDIX F: "Error Rate Equations for the Generalized Biometric System"
APPENDIX G: "Interim IAFIS Image Quality Specifications for Scanners"
APPENDIX H: "Strawman" AAMVA Fingerprint Scanner Quality Specifications
APPENDIX I: ANSI/NIST "Data Format for the Interchange of Fingerprint Information"
APPENDIX J: "WSQ Gray-scale Fingerprint Image Compression Standard"
APPENDIX K: A Fingerprint Survey of AAMVA Jurisdictions
APPENDIX L: "Reconciling Government Use of Biometric Technologies with Due Process and Individual Privacy"
APPENDIX M: Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs
APPENDIX N: Principals for Federal Infrastructure Investment
APPENDIX O: Life-Cycle Cost Analysis

0. EXECUTIVE SUMMARY

0.1 Introduction

In October, 1995, the Federal Highway Administration (FHWA) contracted with San Jose State Univeristy to develop biometric identification standards for possible use with the Commercial Driver's Licensing Information System (CDLIS). (This project was in response to the 1988 Congressional mandate of the Truck and Bus Safety and Regulatory Reform Act (TBSRRA) (Public Law 100-690, Section 9105) for the development of "minimum uniform standards for a biometric identification system to ensure identification of operators of commercial motor vehicles." It follows significant earlier FHWA studies of biometrics, including a 1990 project by the California Department of Motor Vehicles and the Orkand Corporation which investigated the use of fingerprinting and retinal scanning for identifying commercial drivers.) The intent of the 1988 legislation was to promote enforcement of the "one-driver, one-license, one-record" provision of the 1986 Commercial Motor Vehicle Safety Act (CMVSA). It is our intent that the acceptance of this report will place the Secretary of Transportation in immediate compliance with the 1988 TBSRRA legislation mandating biometric standards development for the identification of commercial drivers. (It is not the role of this study to advocate the creation of a biometric system implementing these standards for use in the identification of commercial drivers.)

0.2 The Purpose of the System

Based on our analysis of the House Committee on Surface Transportation Hearings (September, 1987) which lead to the introduction and passage of P.L. 100-690, Section 9105, we believe that the primary intent of Congress was to provide a method of enforcement of the provision in the CMVSA prohibiting the holding of multiple commercial licenses by a single driver. We believe that a secondary intent may have been the detection of counterfeit licenses. In the 9 years since the passage of the TBSRRA, a new problem, that of the fraudulent issuance of a single license to multiple drivers, has surfaced. We believe that a biometric system for the identification of commercial drivers could be an effective means of addressing all of these problems.

We do not believe that Section 9105 limits the development of standards to a predetermined biometric technology, nor do we believe Section 9105 extends to any application beyond commercial drivers licensing. Consequently, this study considered all commercially available biometric technologies for application only to the identification of commercial motor vehicle operators.

0.3 Work Plan

The work plan consisted of the following:

1) Review the legislative and research history of this project;

2) Review all currently available biometric identification methods;
3) Review and revise, as necessary, the 1988 Multi-State Steering Committee functional requirements;
4) Establish a methodology for selecting a technology;
5) Select candidate technologies;
6) Determine, for candidate technologies, which standards exist and which need to be developed;
7) Propose standards for the candidate technologies;
8) Outline a biometric identification system for use with commercial drivers;
9) Perform a rudimentary benefit-cost analysis on the proposed system.

0.4 Technology Selection

We determined that any candidate technology must meet three criteria:

1) be claimed by vendors to support all of the required applications.
2) have been used previously in a similar large-scale application for which an independent performance/cost audit is available indicating that the revised functional requirements can be met.
3) be available from multiple vendors supporting a single image collection, compression and storage standard.

We found that the only technology currently meeting all three of these requirements is electronic fingerprinting. We anticipate no change in this situation over the next decade. We believe electronic fingerprinting to be a fully mature technology, capable of meeting the revised AAMVA functional requirements. Further , we find no technical justification for combining fingerprinting with any other biometric technology

0.5 Standards Development

Standards are required if a biometric identification system is to operate between states or on a national level. Three standards developed by the Federal Bureau of Investigation (FBI), the American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST) currently apply to the use of fingerprinting in large-scale identification applications: the ANSI/NIST Data Format for the Interchange of Fingerprint Information; the FBI's Integrated Automatic Fingerprint Identification System (IAFIS) Image Quality Specification for Scanners; and the FBI's Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image Compression Specification.

These standards were created for "forensic" (criminal investigation) Automatic Fingerprint Identification Systems (AFIS) and, although forming an extremely useful point of departure, cannot be adopted for our use with commercial drivers without extensive review. The primary purpose of forensic systems is to allow the matching of partial "latent" prints, as left at a crime scene, with previously sampled prints from a criminal population, usually rolled onto inked "ten-print" cards. The emphasis is toward identifying every possible candidate print, even if intervention by human experts is required.

In "civilian" (non-forensic) applications, the emphasis is on identifying matches without human intervention and only when the evidence is conclusive, even at the cost of occasionally missing a possible candidate. Only full prints acquired from one or two fingers placed directly on an electronic imaging scanner, not latents, are used, and human intervention occurs only when the computer match on all prints is so conclusive as to constitute evidence of willful fraud.

There are at least four standards required for the application of fingerprinting to commercial drivers:

1) Finger selection
2) Image quality
3) Compression method and ratio
4) Data format

If one application of the biometric system is to be "roadside" identification of the commercial driver, the fingerprint must either be placed on the driver's licensing document or be available using "real-time" electronic transfer from a centralized database. We believe that the placement of the biometric on the licensing document is not secure against professional counterfeiting, even if encryption is used. Consequently, "roadside" applications will require "roadside" data transmission capability. Interstate applications of "roadside" identification will require the development of a fifth standard, one for "feature extraction."

This report only proposes to the Federal Highway Administration reasonable standards such that the Secretary of Transportation will be in compliance with Section 9105 of the TBSRRA. We suggest that the adoption of such standards be done by the American Association of Motor Vehicle Administrators (AAMVA) through their "best practices" procedures, with any modifications as required.

0.5.1 Finger Selection

In May of 1997, seven states collected fingerprints for actual or possible use in their driver's licensing programs. California, Alabama and Hawaii collected right thumbprints. Florida collected left thumbprints. Texas collected both thumbs. Colorado used the right forefinger. Georgia collected both forefingers. As of this writing (October, 1997), both Florida and Alabama have suspended their fingerprint collection efforts.

While it is clear from our study that large-scale identification systems require two fingers, there is no clear choice of which fingers should be used. Thumbs are larger and contain more information. Forefingers are easier to present (ergonomically) and are slightly more varied across the population. We have no scientifically-based information regarding error rate differences among fingers.

Some people, those in social service work for instance, have suggested that the act of fingerprinting a thumb carries a connotation of criminality. For this reason, social service systems universally use forefingers. For technical reasons related to expected false match error rate as discussed in this report, the CDLIS application will require two prints to avoid "candidate lists" (false matches) when matching fingerprints across the current database of 8.5 million licensed commercial drivers. Such candidate lists require human intervention in the decision process and can severely impact the throughput rate of an identification system. Our recommendation is that AAMVA should determine, based on current state use, whether the standard should be for both thumbs or both forefingers.

0.5.2 Image Quality

The Criminal Justice Information Services "Interim IAFIS Fingerprint Image Quality Specifications for Scanners," CJIS-RS-0010v4, Appendix G, (included in this report as Appendix G) specifies requirements for signal-to-noise ratio, gray scale resolution and histogram, modulation transfer function and geometric distortion for fingerprint images scanned into an AFIS. Notably missing from Appendix G are standards for image resolution and size. The resolution standard of 500 pixels per inch is actually included in the ANSI/NIST "Data Format for the Interchange of Fingerprint Information" standard, included in this report as Appendix I. There is no size standard.

These standards were adopted by the FBI after qualitative testing and careful consultation with forensic fingerprint examiners. The goal was to establish the loosest standards compatible with the accurate identification of latent prints by human experts. Several fingerprint companies manufacture scanners to these specifications. The FBI has, in the past, certified scanner performance to Appendix G requirements. Such certified scanners cost around $1000 per unit. The civilian AFIS community has argued that the standards are much stricter than required for non-forensic use, and that cheaper, non-Appendix G compliant scanners can be successfully used for civilian identification. As part of this study, we are proposing a reduced standard, included as Appendix H. Unfortunately, no research data exists on the relationship between image quality and AFIS performance, so we are "guess-timating" when proposing requirements for image quality. We are suggesting that AAMVA develop, based upon this reduced standard, “best practices” for scanner image quality for use in commercial driver identification.

0.5.3 Compression Method and Ratio

In 1992, owing to the pressing problem of large-scale IAFIS data transfer and the noted degradation in expert and computer matching performance when using JPEG-compressed fingerprint images, FBI adopted the Wavelet Scalar Quantization (WSQ) method of compression as the standard, included in this report as Appendix J. WSQ allows for a variable compression ratio for transmission and storage. After qualitative tests with human "latent" examiners, the compression ratio of 15:1 was adopted as the standard. The civilian community believes that higher ratios can be used without catastrophic AFIS performance degradation, but there has been no scientific research in this area. We are proposing that AAMVA adopt WSQ at 20:1 compression as the standard compression method, pending additional scientific studies regarding compression ratio and performance.

0.5.4 Data Format Standard

We propose that the ANSI/NIST "Data Format for the Interchange of Fingerprint Information," included in this report as Appendix I, be adopted, without changes, for use in the commercial drivers licensing project.

0.5.5 Minutiae Extraction

Even fully-compressed fingerprint images are too large to be stored on a licensing document. Almost all commercially available fingerprint systems extract "minutiae" from the fingerprints. Minutiae are, roughly speaking, the location of the ridge endings and ridge "bifurcations" (splits) in the fingerprint. Beyond this, however, there is no agreement among AFIS contractors as to what other information should be contained in the minutiae record. Most contractors differentiate between ridges and bifurcations, and add the angle of the ridge at the minutiae point. The amount of additional information that can be added is virtually endless, and minutiae records can be from 26 to 1000 bytes long. The fingerprint image cannot be reconstructed from the minutiae record. Matching is done by comparing the minutiae points to those extracted from previously stored prints. There is no scientific research available regarding AFIS performance and minutiae record size or content.

There are no government standards for defining minutiae records or their extraction or storage. This means that minutiae records stored on a licensing document will not be usable across system contractors. Unless every state contracts with the same contractor, inter-state "roadside" driver identification is not feasible with records stored on the document. Early in 1997, NIST held informal meetings with the AFIS industry on this issue, but no immediate progress was been made. Owing to vendor pride and "proprietary" approaches, minutiae standardization is proving to be a very difficult and daunting problem. We recommend that AAMVA attend any minutiae standards meetings held by NIST. We do not recommend that FHWA or AAMVA directly attempt to establish such standards.

0.6 Three System Designs

There are three ways of approaching the creation of a nationwide biometric system for identifying commercial drivers. The general nature of this system is independent of the choice of fingerprinting as the candidate biometric technology, but is highly dependent upon funding, politics and the Federal prerogatives/states' rights debate.

0.6.1 The Centralized System

The most straightforward and cheapest approach to the identification of commercial drivers would be a national system, much like CDLIS, which electronically holds the minutiae records of all licensed commercial drivers. The minutiae would be "pointers" by which the database could be accessed. Recalling that fingerprint images cannot be reconstructed from the minutiae records, the original images would remain stored in the states which collected them and accessed only if a prosecution for drivers licensing fraud was indicated. However, because each state might be using different fingerprinting contractors with incompatible minutiae record formats, the fingerprint images, collected during the licensing procedure using scanners of standardized image quality, would need to be transmitted in compressed form to the central site for minutiae extraction. The states would archive the images, while the central site would extract the minutiae, then discard its copy of the original images. States objecting to the transmission of compressed images could send the minutiae only, but would be required to use the contractor-specific minutiae extraction software mandated by the national system manager.

A commercial driver applying for a new license or a renewal would have copies of his/her images sent to the central site, converted to minutiae and scanned against the existing database. The transmitted copies of the images would then be destroyed. In the case of a new license, if no match was found, the license could be issued and the minutiae stored in the database. In the case of the issuance of a duplicate or a renewal, a match should only be found against the registered license holder. Any other matches would indicate multiple license fraud. This approach to scanning the entire database for both new licenses and renewals provides a "double check" against multiple issuances. To be effective, all states would be required to participate. A non-match during the renewal or duplicate issuance process might indicate single license/multiple driver fraud.

Could such a large centralized system be built and would it work? Scientific information on large-scale system performance has recently come available from an international AFIS contractor benchmark test conducted by the Philippine government. An important feature of large-scale AFIS systems is that of print classification to decrease the required scope of the search. Stored prints are classified as to "arch," "whorl," etc. (or into some other groups). When a sample print is received for comparison, it is likewise classified, then compared only to those prints with the same classification. Two-print systems can, on average, match prints by comparison with only about 10% of the stored prints in the total database. The measure of this efficiency increase is known as the "penetration rate." Assuming 8.5 million commercial drivers (some of whom may be inactive and not seeking renewal), with approximately 3 million renewal, state transfer and new licenses annually, 240 20-hour work days annually at the central site, two-finger matching and a 25% penetration rate, about 400,000 comparisons per second would be required. Although no system of this size currently exists, it is within the capability of current contractor designs.

Compressed images are about 15 kbytes in size. This data can be transmitted over standard modems in two or three seconds and could be sent to the central site over AAMVANet or internet lines. The data arrival rate at the central site (over an 11-hour national work day) would be about one 15 kbyte image (plus data format header and overhead) every 3 seconds, requiring trivial input bandwidth.

Current system performance appears to be highly contractor dependent, false match errors occurring perhaps once in every 10 million comparisons. Assuming independence of errors, two finger false matches would occur about once every 10^{14} matches. Using the same numbers as in the paragraph above, this would equate to a false match every few decades.

False non-matches occur at a rate of 2% to 10% per single finger comparison. Again assuming independence of errors, two finger false non-matches would be less than 1%. This number has to be interpreted carefully. It means that less than 1% of all persons attempting fraud through random means will be successful, while 99% will be caught.

0.6.2 The Distributed System with Centralized Communication

A second approach would be to have each state maintain and control its own commercial driver AFIS system. Each state could have a different contractor and different minutiae extraction protocols, but each would collect data at the nationally-mandated image quality standard. Duplicate or replacement licenses would be issued only upon the verification against the state's own database of the applicant's fingerprint. Single license/multiple driver or driver substitution fraud could be detected with no interstate transfer of data.

When a driver applies for a new license, the compressed fingerprint image would be sent by AAMVANet, NLETS or internet to a centralized communication site for distribution to the independent systems in all the other jurisdictions. Any jurisdiction finding a match would report the find directly to the originating state.

The centralized communication site would have to transmit each image 50 times, leading to a centralized output of several hundred kbytes per second, a trivial load for a large server. Input data rate at the state and central sites would be at the average rate of one image every 3 seconds. California, the largest state with about 600,000 commercial driver's licenses (CDLs), would be conducting about 50,000 comparisons per second (considering a 25% penetration rate), requiring a mid-sized system.

The political advantage of this system is that states would only release images for immediate search, not for storage in any form outside the state. Each state would maintain complete control of all its images and derived minutiae. The disadvantage would be the total cost of the system, with loss of the economies of scale of the centralized system. The effectiveness of this system would be identical to the centralized system, provided that all states participated.

0.6.3 The Distributed System with Direct Communication

The third approach is identical to the second, except that compressed fingerprint images would be sent directly by the collecting state only to selected, participating states for search. Receiving states could charge a fee for searching of an image against their database. This would require no generalized transmission of fingerprint images, giving each state tight control over which images would be sent to which states for search. Further, states could participate or not in this system as local politics required. This system would be effective against renewal and single-license/multiple-driver fraud. Effectiveness against multiple license fraud would be limited, however, if not all states participated.

0.7 Legal Considerations

We have determined that there are several Constitutional principles potentially linked to a government requirement for the submission of a biometric measure as a prerequisite for the issuance of a driver's license. These are: due process, search and seizure, and self-incrimination, as well as the implicit right to privacy. Our survey of legal challenges to government-required submission of a biometric identifier revealed several pertinent court rulings, nearly all of which upheld the practice when justifiable on grounds of public safety.

The most directly applicable case was *Christopher Ann Perkey v. Department of Motor Vehicles,* decided by the California Supreme Court. California instituted a requirement that each applicant for a driver's license submit a fingerprint to the Department of Motor Vehicles. Ms. Perkey refused to be fingerprinted and was denied a license solely on the basis of this refusal. She took legal action, claiming that the fingerprint requirement violated substantive due process because there was no relationship linking it with the state's stated interest in promoting highway safety.

The California Department of Motor Vehicles asserted that fingerprint technology was the only reliable way to ensure the integrity of its drivers licensing records and that the interception of applications from those who pose a serious danger to public safety constituted a proper legislative objective. The California Supreme Court agreed that the fingerprint requirement bore a rational relationship to the legitimate goal of furthering highway safety by giving the state a reliable method of checking the identity of driver's license applicants and upheld the requirement for fingerprinting.

Although this finding only applies in California, government required physiological sampling has been upheld by several U.S. Supreme Court rulings against several challenges. In the case of *Breithraupt v. Abram*, decided in 1957, police took a small blood sample from an unconscious person involved in a fatal car accident. The Supreme Court ruled this extraction was constitutionally permissible, stressing that clinical blood extraction was not significantly intrusive and had become both commonplace and accepted by society. Nine years later, the Court reiterated this point in *Schmerber v. California*, by recognizing that both federal and state courts have held that the right against forced self incrimination does not extend to forced subjection to fingerprinting, photographing, or physical measurements, nor to forced writing, speaking, standing, walking or gesturing for identification purposes.

Our research indicates that a requirement for fingerprinting as a prerequisite for the issuance of a commercial driver's license would most likely be upheld in a court challenge.

The greatest legal challenge to such a system will be from the states themselves. Of the four states currently collecting fingerprints electronically, one (Georgia) would be unable to release those prints to other states under current state law. One (California) would be unwilling to release their prints to a federal system without mandating federal legislation. Most states not currently collecting fingerprints would require modifications to state law, or a federal mandate, to begin collection.

0.8 Benefit-Cost Analysis

Our study includes a procedure for a detailed benefit-cost analysis. Estimating the financial costs of any of the three designs given above is not difficult. Industry sources indicate that the centralized system could be built for under $15 million. Total cost of the distributed system would be greater, owing to the loss of economies of scale, but capital expenditures of each state would be at most a few million dollars.

The primary problem we face is in estimating the financial benefits of the system, particularly in the absence of any conclusive evidence that the current system for enforcing the "one-driver, one-license, one-record" is ineffective. In November, 1996, the New York State Department of Motor Vehicles completed the "Multiple CDL Study" for the Federal Highway Administration. According to this study, "the multiple CDL problem has decreased to the point that it appears to be virtually non-existent." Further, the study states, "Although potential duplicates (CDLs) surfaced in our records comparison results, the numbers were statistically insignificant."

We know of no documented, post-CMVSA case of a commercial driver actually having two commercial licenses. On the other hand, anecdotal evidence[1] has recently emerged from the Alabama Department of Public Safety that a problem may exist with multiple drivers sharing a single license. This issue was not addressed by the "Multiple CDL Study" and, consequently, we have no estimates of the size of this related problem. The use of biometric identification with the CDL, specifically the on-line availablilty of the biometric record with the driver data in the CDLIS database, could eliminate the problem of multiple drivers on a single license.

[1] The State of Alabama is currently pursuing a criminal investigation in the "Leon Carmichael" case, in which one of several drivers fraudulently carrying a single Alabama CDL was killed in a motor carrier accident in Utah.

Pending the completion of current, on-going studies,[2] it is difficult to estimate traffic safety benefits to be accrued from the deployment of a biometric identification system for commercial drivers owing to the lack of hard data on the size of the commercial driver authentication problem. Nonetheless, we have included in our study a detailed analysis of what types of data would be necessary to support this project from a benefit-cost perspective.

0.9 Conclusions

This study recommends that fingerprinting be established as the biometric for identifying drivers pursuant to Section 9105 of the "Truck and Bus Safety and Regulatory Reform Act." This study further defines the minimum required scope of the system and recommends specific "minimum uniform standards" for the biometric identification of commercial drivers using fingerprinting. We have included results of a recent large-scale fingerprinting test showing the feasibility of two-finger systems at a scale comparable to the current CDLIS enrollment.

We suggest several standards (scanner image quality, compression, data transmission format) for adoption by AAMVA as "best practices" and outline several system approaches for using biometric fingerprint technology to enforce the "one-driver, one-license, one-record" mandate of the Commercial Motor Vehicle Safety Act. In the absence of hard information supporting the existence of a problem with multiple licenses or single licenses with multiple drivers, we have difficulty in computing the benefit-cost feasibility of such a system, but have included a computational methodology for use as such data becomes available.

We recommend that the FHWA cooperate with AAMVA to establish "Best Practices" for biometric identification using the fingerprint, including standards for finger selection, scanner image quality, compression technique and data transmission format, based on the specific recommendations of this report in these areas. We further recommend that AAMVA create model fingerprint collection and protection legislation to serve as a guide for states wishing to begin the fingerprint identification of commercial drivers.

[2] Two relevant projects are currently being undertaken by AAMVA: the CDLIS/Social Security Administration Verification Study and the TML/AAMVA CDL Effectiveness Study.

1.0 THE HISTORY OF THE FHWA BIOMETRIC IDENTIFICATION STANDARDS PROJECT

The current project funded by the Federal Highway Administration, Office of Motor Carriers (FHWA-OMC), to study the use of biometrics for the identification of commercial motor vehicle drivers, is not the first FHWA study to address this issue, but rather is one more part of an initiative started 10 years ago by Congress to improve the safety of commercial vehicles and their operators on our nation's highways.

In 1986, the US. Congress passed the Commercial Motor Vehicle Safety Act[3] (CMVSA) establishing a "one-driver, one-license, one-record" policy for commercial drivers. To enforce the act, which made it illegal for a commercial driver to be licensed concurrently in more than one state, the Commercial Drivers License Information System (CDLIS) was established, becoming operational in the early 1990's.

1.1 House Subcommittee on Surface Transportation Hearings (1987)

On September 16, 17 and 23 of 1987, the US House of Representatives Subcommittee on Surface Transportation held hearings, for the purpose of oversight of the CMVSA, which ultimately lead to the Truck and Bus Safety and Regulatory Reform Act (TBSRRA) of 1988.[4] At the September 16 meeting, Thomas Donohue, President and CEO of the American Trucking Association (ATA) presented both written and oral testimony on the subject of biometric identification of commercial drivers. The ATA written testimony stated:[5]

> "If the commercial driver's license program is to be effective, there must be a means of assuring that each individual license holder is properly identified and cannot falsify identity to obtain additional licenses. Without this 'unique' identifier the program cannot be totally successful.
>
> The Act requires basic information for licensees such as name, address, description and social security number. It gives the Secretary of Transportation the option of requiring a different identifier than the social security number. It is generally recognized, even by those who advocate the social security number as an identifier, that a commercial driver can have more than one such number, and that social security cards can be counterfeited or otherwise falsified.
>
> On the other hand, there are systems which use 'unique identifiers' such as fingerprints or retinal images, which are much more reliable and should be used in the licensing system to make identification foolproof. ATA has

[3] Public Law 99-570, October 27, 1986

[4] "Truck and Bus Safety and Related Issues: Hearings before the Subcommittee on Surface Transportation of the Committee on Public Works and Transportation House of Representatives (100-28)", US Government Printing Office, Washington, DC., 1988

[5] Ibid, pg. 54-55.

> seen demonstrations of these systems and is impressed. They are in use, now, by government and private sector organizations. Yet, DOT has apparently decided to utilize social security numbers as the unique identifiers and has placed the other systems on the back burner for further research.
>
> While DOT is apparently satisfied with the status quo of social security number identifiers, it has not publicly stated why it believes that the more effective systems of fingerprints and retinal images cannot be used. Given the importance of the identifier to the success of the commercial driver's license program, ATA believes that DOT should provide the leadership and expedite a program for utilization of these identifiers....
>
> If DOT does not quickly establish a program for utilization of effective identifiers, commercial drivers will continue to falsify their license applications and spread their driving violations among several licenses."

In his oral testimony, Mr. Donohue was questioned on biometric identifiers for commercial drivers by Rep. Dennis Hastert of Illinois. The exchange was recorded as follows:[6]

> " Mr. Hastert: But there are multiple licenses, aren't there, assigned?
> Mr. Donohue: But there won't be, Congressman, if when we give out the license, we have an identifier on it, and we can argue what that identifier is, let's say for the sake of argument, it's...
> Mr. Donohue: So let's say it's a retina identifier, just for argument's sake...You get three moving violations of significance, and the state pulls your license. Now you don't have a license. You can go to any state in the Union and apply for a license, they take the retina, they run it through the national clearinghouse, and they say, 'Don't give him a license'."

1.2 The Truck and Bus Safety and Regulatory Reform Act of 1988

The resulting "Truck and Bus Safety and Regulatory Reform Act"[7] (TBSRRA) passed by Congress in 1988 contains the following section:

> "Sec. 9105. Biometric Identification System
> (a) REGULATIONS.--Not later than December 31, 1990, the Secretary shall issue regulations establishing, for purposes of sections 12007[8] and

[6] Ibid, pg. 32-34

[7] Public Law 100-690, November 18, 1988

[8] Section 12007 of the CMVSA, titled "Commercial Driver's License Information System," establishes the specifications for CDLIS.

12009[9] of the Commercial Motor Vehicle Safety Act of 1986, minimum uniform standards for a biometric identification system to ensure identification of operators of commercial motor vehicles.
(b) PILOT DEMONSTRATION PROJECT.-- To carry out a pilot project to demonstrate the use of biometric identification systems for ensuring identification of operators of commercial motor vehicles, the Secretary may use not to exceed in each of fiscal years 1989 and 1990 --

(1) $500,000 from the funds made available to carry out section 402 of the Surface Transportation Assistance Act of 1982; and

(2) $1,000,000 from the funds made available to carry out section 12010 of the Commercial Motor Vehicle Safety Act of 1986."

1.3 The Multi-State Steering Committee's Functional Requirements

In 1988, to comply with section 9105 of the TBSRRA, the FHWA funded the State of California Department of Motor Vehicles (CA-DMV) to conduct a study of biometric identification technologies for the purpose of identifying commercial motor vehicle drivers. The FHWA, as a condition of this grant, required the CA-DMV to create and chair a committee of states known as the "CDL Biometric Identifier Multi-State Steering Committee"[10] (MSSC). Working without the availability of vendor-independent data on the performance of biometric devices in this application, the MSSC established a list of 16 functional requirements describing an acceptable biometric identification system.[11] This list is given in its original form, and with revisions suggested by the 1997 American Association of Motor Vehicle Administrators (AAMVA) Biometric Working Group, in Section 5 of this report.

In the subsequent CA-DMV study, the following subset of the original functional requirements were considered:[12]

"Data Collection Related:

- Biometric collection systems must provide on site, local quality control.
- Capture method must be unobtrusive and socially acceptable.
- Data capture time should not increase net transaction time by more than 30 seconds.
- Capture method must be simple to use by both employees and customers.
- The system must be reliable.

[9] Section 12009 of the CMVSA, titled "Requirements for State Participation," allows the federal government to withhold funds from States not meeting specified minimum standards for the issuance of commercial driver's licenses.

[10] The Orkand Corporation, "Personal Identification Project: Technical Report Final," May 16, 1990, DMV 88-89, pg. ES 1. This report has been reprinted with permission of the original authors and is available from San Jose State University College of Engineering.

[11] State of California Department of Motor Vehicles, "Personal Identifier Project: Feasibility Study Report," Project No. 2300-75, Log No. 215-88, December 7, 1988 revision.

[12] Ibid, pg. ES 2-3.

Data Processing Related:

- Biometric identifier must be accurate.
- Error rates must not exceed .5% when impacting the proper issuance or refusal of an original or renewal license.
- The system must perform without a candidate list for 99.9% of the inquiries.

Industry Related:

- Any system must meet data exchange standards recognized by AAMVA both now and in the future and, for fingerprints, ANSI standards."

1.4 The Orkand Studies

In 1988, an award was also made by FHWA to the Orkand Corporation to recommend candidate biometric technologies and to structure a demonstration project.[13] This report concluded that fingerprinting and retinal scanning were the two most promising candidate technologies.

CA-DMV subcontracted with the Orkand Corporation to perform the demonstration project. Approximately 31,000 records each of fingerprints and retina scans were collected at motor vehicle offices in California, Texas, North Carolina and Illinois. The fingerprint data was collected using both inked rolled prints and "live scan" devices with no front end quality control. The study was divided into four tests: two enrollment tests for correct issuance and correct denial of a license; and two verification tests for correct matching and non-matching of a applicant with an existing record. Error rates for the four tests of the two technologies varied from 0-16% and were attributed to "data collection" and "data processing" errors.

The study concluded in 1990, stating that "fingerprint technology more nearly meets the goals established for a CDL biometric identification system..." The full final report has been reprinted by San Jose State University, with permission, for general dissemination.

1.5 Advanced Notice of Proposed Rule Making 1989 and the 24 Questions

In 1989, prior to the release of the final CA-DMV report, the FHWA released an Advanced Notice of Proposed Rulemaking[14] (ANPRM) listing 24 issues and questions for comment. These were:

1) How many drivers currently operate in defiance of the law?

[13] L. Wenchel and D. Forsburg, "Functional Description for a Unique Identification System for the Commercial Driver's License Information System," Report MC-88048, The Orkand Corporation, Silver Spring, Maryland, February 1988

[14] "Minimum Uniform Standards for a Biometric Identification System to Ensure Identification of Operators of Commercial Motor Vehicles," Federal Register, Vol. 54, No.92, May 15, 1989, pg. 20875-20879

2) How extensive will this problem be when the program is fully implemented and all CDL holders are entered into the CDLIS?
3) On what basis are the above estimates of the size of the problem made?
4) What alternatives besides the biometric identifier can be used to reduce or eliminate the problem?
5) Since the CDLIS supports a broad comparison of identifying information, does internal comparison of individual identification records, in conjunction with severe penalties, provide ample reason for drivers not to seek multiple licenses?
6) How much will such a system cost in terms of hardware, software, personnel, training, and impacts on existing state licensing procedures?
7) What factors are most likely to increase costs of the system?
8) What are the costs likely to be for making the system mandatory for all states as opposed to making it optional?
9) What are the benefits likely to be? a) In terms of money? b) In terms of "non-monetary" or social benefits?
10) How much would each state be willing to pay each year for such a system? a) In terms of additional AAMVAnet costs? b) In terms of within state costs? c) Both of these?
11) How much would each licensee be assessed for such a system and how would this relate to total costs?
12) What is a tolerable error rate for both erroneously identifying a match when there is not one and not identifying a match that should actually be one?
13) How much additional time for conducting the match search is considered acceptable?
14) Under what conditions would it be acceptable to issue temporary licenses?
15) What are the acceptable added costs per license, assuming limited and widespread use?
16) What benefits would be achieved in having the biometric information available on the CDL in a form that could be read electronically?
17) Should the establishment of such a system be made mandatory for all states?
18) If so, when should such a system be mandated?
19) Are there privacy issues involved?
20) Would there be any privacy distinctions between an AFIS and the retinal scan?
21) If problems are noted, what modifications would alleviate these?
22) Who should have access to this data and for what purpose?
23) Is there vendor support to accommodate nationwide implementation and projected growth?
24) Should the FHWA merely specify performance parameters and leave vendors to develop requisite systems, or should the selection be restricted to existing system designs?

Our response to all of these questions is given in Section 13 of this report.

1.6 Public Response

After publication of this ANPRM, FHWA received seventeen comments from the general public, trucking industry and labor representatives, several states, and the National Transportation Safety Board (NTSB).[15] The NTSB and the American Trucking Association (ATA) "expressed strong support for the expeditious adoption of a biometric identifier." The ATA favored retinal scanning over fingerprinting and encouraged biometric capability at roadside inspection sites. The Teamsters' Union and the Owner Operator Independent Drivers' Association (OOIDA) "expressed equally strong opposition...as did (an) individual driver." The Teamsters' wrote, "The safety benefits of 'catching' or deterring multiple license use in this small number of drivers must be considered in view of the monetary, time, 'hassle' and privacy costs." The OOIDA opposes "measures that single out truck drivers to be automatically treated as criminals with no benefit to highway safety" and is concerned about use of biometric identification to harass drivers at roadside inspection stations. The ten states that responded

> "wanted the FHWA to provide additional time...to more fully assess the costs and benefits of a biometric system. Most wanted to be sure that error rates were very low; the rates suggested by the various states ranged from a high of less than five percent, to lows of a general error rate of less than one in 1000, no more than one significant match problem per month, or simply an overall error rate of zero. Some states that issue licenses over the counter generally were concerned about response time...the overall sentiment expressed in comments from the states was a desire to wait until the CDL program is well underway before requiring a biometric identifier."

1.7 Advanced Notice of Proposed Rulemaking 1990

Upon the conclusion of the CA-DMV study, the FHWA contemplated issuing a "Notice of Close-Out of the Biometric Identifier Rulemaking," but rather, prior to publication, changed the title to "Advance Notice of Proposed Rule Making: Additional Information." This notice[16] summarized the CA-DMV findings and concluded

> "The pilot study clearly shows that neither of the systems meets the functional requirements set forth in the "Feasibility Study Report." While the accuracy associated with the AFIS system is better than that of the retinal scan, improvement is still necessary to meet the criteria recommended by the CDMV and the committee of states.

[15] "Minimum Uniform Standards for a Biometric Identification System to Ensure Identification of Operators of Commercial Motor Vehicles: ANPRM; additional information," Federal Register, Vol. 56, No.46, March 8, 1991, pg. 9925-9928

[16] Ibid

> Further cost estimates are also needed. Decisions concerning the type and configuration of the system may need to be made before these can be completed.
>
> ...information is needed concerning the effectiveness of the current system of identifying drivers within the CDLIS, including estimates of how many drivers attempt to circumvent, and succeed in circumventing, the current system and receive more than one commercial driver's license. This information is needed before the costs and benefits of a biometric system can be determined.
>
> It is also clear that more time is needed so that the technology has an opportunity to develop to meet the functional requirements....It may be desirable to review some of the functional requirements in the light of the continuing experience with biometric technology and evolving needs of the states....the FHWA will complete and make available the results of several studies designed to address the effectiveness of the current identification system...
>
> The development of biometric technology will be closely monitored...the FHWA will consider research, controlled testing and other appropriate measures to help determine when technology will be available to meet the needs of the states. When information is available to show that a biometric identifier would be beneficial to the CDL program and the technology has been developed, or can be developed, to meet appropriate functional requirements, the FHWA will propose standards for a biometric identifier."

1.8 The Broad Agency Announcement of 1995

In April of 1995, the FHWA issued a broad agency announcement seeking a contractor to perform "Biometric Identifier Standards Research"[17] which contained the following paragraph:

> "Biometric identifier standards research. This project will review the current status of biometric technologies to determine their ability to meet the needs of the Commercial Driver's License (CDL) program. Also, it will seek to determine the cost-effectiveness of the most promising technologies for large scale applications. Model biometric identifier standards will be developed for these identifier technologies for use in the CDL program. These standards will be used as the basis for a proposed rulemaking to establish minimum standards for the state

[17] FHWA, "Broad Agency Announcement (BAA) for Commercial Motor Vehicle Driver Human Factor Research," SOL DTFH61-95-R-00117

> driver licensing agencies that decide to use biometric identifiers to enhance their CDL programs. Study responds to Congressional mandate in Section 9105 of the Truck and Bus Safety and Regulatory Reform Act of 1988 to establish minimum uniform biometric identifier system standards for the CDL program. ($400,000)"

1.9 The San Jose State University Proposal

San Jose State University responded to the FHWA BAA and was awarded a contract based on a proposal[18] to perform the following work:

> "Our specific proposal is for an 18 month, 3 person-year effort in five iterative (as opposed to sequential) stages:
>
> 1) Review the CA-DMV feasibility and demonstration studies and all other FHWA efforts addressing implementation of PL 100-690, Section 9105;
> 2) Review and revise the Steering Committee's functional requirements to consider both state level and CDLIS use of biometric identifiers;
> 3) Review all current biometric technologies with regard to the revised requirements;
> 4) Determine potential cost effectiveness of selected candidate technologies;
> 5) Develop model standards for use and performance of devices in application to state level programs and CDLIS, based on the revised functional requirements;"

The San Jose State study is divided into several sub-tasks. We have worked with the FHWA and AAMVA to: 1) define, specifically, the application of biometrics technology to the national commercial driver's licensing system; 2) establish a general methodology for determining the best biometrics technology for any specific application; 3) establish criteria for selecting candidate technologies for this application; 4) select candidate technologies; 5) suggest candidate standards for a multi-state system based on these technologies; 6) obtain cost and operational data from existing systems employing these technologies in a similar application; 7) discuss implementation issues, such as system design, cost/benefit, and estimated system performance.

2.0 BIOMETRIC TECHNOLOGIES AND THE INTENT OF CONGRESS

The primary objective of this study is to make recommendations to the Secretary of Transportation on the establishment of "minimum uniform standards for a biometric identification system to ensure identification of operators of

[18] San Jose State University, "Proposal to Biometric Identifier Standards Research: in Response to BAA/RFP DTFH61-95-R-00117," July 1995

commercial motor vehicles," as required by Section 9105 of the 1988 Truck and Bus Safety and Regulatory Reform Act (TBSRRA), as given in full in Section 1.2.

We define "biometric" technologies as "automatic methods for the identification, or identity verification, of individuals based on physiological or behavioral characteristics." We believe this definition is compatible with the meaning of the term as used in the TBSSRA. There are various technologies in each group. The behavioral technologies include automatic signature verification, keystoke analysis, and voice recognition. The more numerous physiologically-based systems include finger and palm prints, hand and finger geometries, eye (iris and retinal) scans, facial images and thermograms, vein patterns, and even body odor systems. Despite the references to fingerprinting and retinal scanning in the Congressional hearings documented in Section 1.1, we believe that Congress did not intend Section 9105 be restricted ***a priori*** to any particular technology. Consequently, this study considered all commercially available biometric systems.

More problematic in interpreting Section 9105, however, is discovering the policy rationale for the system. As to be discussed in Section 16.1.2, this rationale is now required by Office of Management and Budget for the justification of federal programs. From the wording of Section 9105 alone, we cannot easily determine the precise scope of the application intended by Congress However, it is abundantly clear from the text of the law and the sub-committee hearings that Congress had absolutely no intent of extending the scope of this study beyond its mandate "To regulate Commerce... among the several States," as provided in Article I, Section 8, Clause 3 of the U.S. Constitution. Consequently, this report does not consider in any way the application of biometric technology to the identification of non-commercial drivers.

We believe that there are functionally several ways that a biometric system could "ensure identification of operators of commercial motor vehicles" within the intent of Section 9105. A system could prevent, detect and/or deter the holding of a fraudulent commercial license, and/or it could prevent, detect and/or deter the holding of multiple commercial licenses by a single driver. Section 4 of this report will attempt to articulate more clearly the possible functions.

At the onset of this project, there was no commonly accepted method for describing or differentiating biometric applications. Three papers, included in this report as Appendices A, B, and C, explain the application classification scheme developed for this project and the relationship between system function and the suitablility of the various biometric technologies. To summarize the approach, applications of biometric technology can be partitioned in several ways:

1) Cooperative vs. Non-Cooperative. Is the strategy of the bad guy cooperation or non-cooperation with the system?
2) Overt vs. Covert : Do the users know that biometric information is being extracted?

3) Habituated vs. Non-Habituated: Are system users familiar and comfortable with the usage of the system?
4) Attended vs. Non-Attended: Is system use supervised by an agent of the system manager?
5) Standard vs. Non-Standard Operating Environment: Is the equipment being used in an office environment, or outdoors?

This list is open, meaning that additional partitions might also be appropriate. The most important conclusions derivable from this approach are that: 1) only physiologically-based technologies can be used in non-cooperative applications, because consistent human behavior cannot be mandated; and 2) obtainable performance, in terms of error rates, depends upon the taxonomy of the application.

The several applications believed to be within the intent of Congress in creating Section 9105 of the TBSRRA are of differing taxonomies. These are presented in Section 4, after a brief discussion on biometric systems, in general.

3.0 A PRIMER ON BIOMETRIC SYSTEMS

All biometric systems have the common function of identifying individuals by matching some personal characteristic with one previously recorded. The methods and uses of biometric systems vary widely, however. Primary to the development of biometric standards is an understanding of the normative system model common to most biometric technologies in most applications. Certainly not all biometric methods will fit any single model, but tremendous insight can be gained by noting where individual systems differ from the norm. Figure 1 shows a system diagram of the general biometric system. Five sub-systems are shown: data collection, transmission, signal processing, storage and decision. In the following sections, we will describe each sub-system in detail.

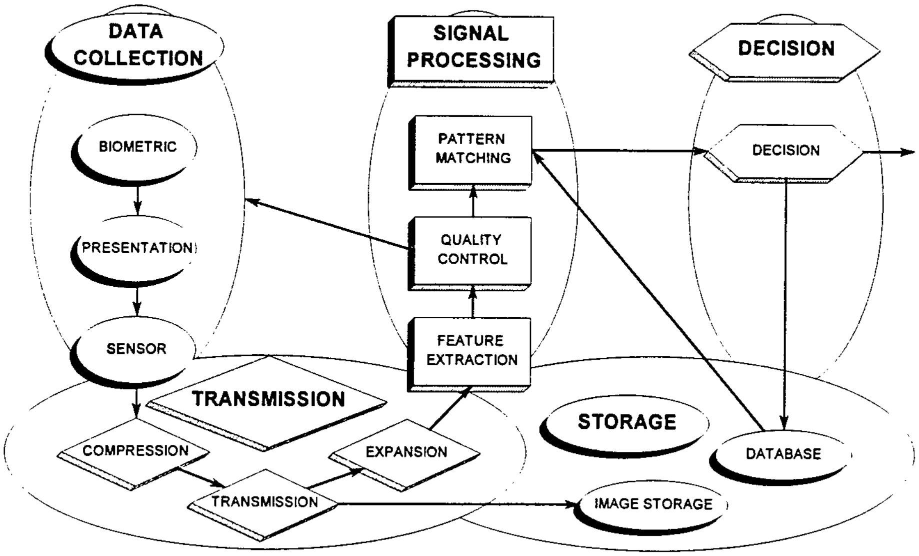

Figure 1: The General Biometric System

3.1 The Data Collection Sub-System

The data collection sub-system samples the raw biometric data and outputs a one- or multi-dimensional signal. The input biometric pattern needs to be fairly stable over the time period of interest, which in the case of commercial driver's licensing is about four years. Even if the fundamental, targeted patterns (finger ridges or iris patterns or retinal vasculation) are stable for life, injury or disease may cause changes in the observed patterns. Some patterns, such as voice, face or signature, simply drift, although perhaps reversibly.

The biometric pattern is "presented" to a sensor, which transduces the pattern into an electronic signal. Most biometric systems expect a "standardized," predetermined presentation of the pattern. The sensors must be as stable as possible, meaning that we hope that all sensors in the system will have similar performance measures and, for a single sensor, re-calibration will not often be required. Some sensors have the capability of determining whether or not a signal of acceptable quality has been acquired. In other systems, quality control is exercised by the signal processing sub-system. The presence of automatic quality control at some stage of the process is not currently present in all biometric systems, at the expense of higher than necessary false non-match rates.

So, we can see that the output of the data collection sub-system is impacted by changes in: 1) the underlying biometric pattern; 2) the presentation of the pattern; 3) the sensor device. Changes from any or all of these sources ultimately result in recognition errors.

3.2 The Transmission Sub-System

Many biometric systems collect data in one physical location and process it in another. To minimize required transmission bandwidth, data compression may be required. The signal processing sub-systems downstream are designed to process the original image, so expansion of the compressed image is always required prior to processing. Compression/expansion may be "lossy" or "loss-less" with regard to the quality of the expanded signal, but lossy compression algorithms generally result in much greater bandwidth reduction.

Compression/expansion algorithms are designed and tested to work well on signals of an expected quality. If the sensors transducing the original signal do not meet the expected technical quality requirement (lower sampling rate, for instance), losses during the compression/expansion process may be unpredictable. The transmission channel may also add noise, particularly if analog signals are used, leading to increases in recognition errors. If storage of the raw biometric pattern is required, storage can be in compressed form to save space.

3.3 The Signal Processing Sub-System

The signal processing sub-system takes the now degraded image of the original biometric pattern and converts it into a "feature vector"[19], also called a “template”. The intent is to distill into this vector the information in the original biometric data that is time-, presentation-, sensor-, compression- and transmission-invariant. Clearly, these algorithms are always highly proprietary. They all share the property of being non-invertible, meaning that **the original pattern cannot be reconstructed from the feature vector.** This inherent property of all biometric methods will have important ramifications in our standards development task.

Systems not using quality control at the sensor can perform a quality analysis in the signal processing sub-system. If quality analysis indicates that the received pattern was of satisfactory quality, the feature vector is passed to the pattern matching module, where it is compared to some number of stored feature vectors, one by one. This comparison results in a numerical measure quantifying the degree of similarity or difference between the compared patterns. This value is sent on to the decision sub-system.

At this point, there emerges a difference between enrollment and operation in the activity of the signal processing subsystem. For enrollment, if the policy is to accept any enrolled pattern, the feature vector is passed directly into storage with no pattern matching. If the enrollment policy is to accept only enrolled patterns that do not closely match any already in the database, the pattern matching module will be called on to compare the feature vector with potentially matching feature vectors previously stored in the database. All similarity measures developed during this process will be passed to the decision module. This process is also known as "identification." The difference between this and the "verification" operation is that, for verification, the searched portion of the database is confined to a single pattern, so only a single comparison measure is passed on to the decision module.

Additional information is often available to the system that can be used to limit the number of required comparisons when searching the database. This information path is not indicated in Figure 1, as it can be highly variable between systems. In the case of "verification," the additional information may be a "claimed identity" in the form of a name or an identification number narrowing the comparison to a single stored pattern; or the database may be on a "smart card" containing but a single enrolled feature vector (template). In the case of "identification," the number of required comparisons may be limited by external information, such as the age of the customer, or by information endogenous to the biometric sample itself, such as the fingerprint pattern type. In any case, the actual activity of the signal processing system is exactly the same: extraction of the feature vector, checking of quality, and comparison of the feature vector to some number of enrolled vectors.

[19] Generally, these features are indeed "vectors" in the mathematical sense, fingerprint minutiae being the notable exception.

3.4 The Storage Sub-System

We have already implied that two types of data might be stored in the storage sub-system: compressed biometric patterns and enrolled feature vectors (templates). Because the feature vector extraction process is non-invertible, the biometric patterns must be stored if their recovery will ever be required. The biometric patterns cannot be recovered from the feature vectors. Also as previously indicated, to limit the number of comparisons, the templates may be partitioned in the database on the basis of additional information collected with the biometric data, such as gender.

3.5 The Decision Sub-System

The inputs to the decision sub-system are the measures resulting from each comparison of a feature vector to a stored template. The purpose of the decision sub-system is to invoke the system decision policy. If the measures indicate a close relationship between the feature vector and one of the compared, stored templates, a "match" is declared. If none of the measures indicate similarity, a "non-match" is declared. Beyond this, the differences between system decision policies are so great that little, in general, can be said.

The system activities resulting from a "match" and "non-match" may also vary greatly according to application and decision policy. For instance, during enrollment in driver's licensing applications, a "non-match" results in the "acceptance" of an applicant into the system. For "roadside" verification of the registered relationship between license presenter and document, however, a "non-match" results in the "rejection" of the driver. In systems using biometric patterns subject to significant drift, the "matching" of a sample with an enrolled template may result in the updating of the stored template with the new sample.

4.0 SYSTEM APPLICATIONS AND FUNCTIONS

We believe Section 9105 can be currently interpreted to target two potential problems: multiple and fraudulent commercial licenses held by any commercial driver. For each application, the system might have as many as three goals: prevention, detection and deterrence.

4.1 System Alternatives

One application is the prevention, detection and deterrence of the possession of multiple commercial licenses by a single driver. Based on our interpretation of the hearings of the Subcommittee on Surface Transportation, as discussed in Section 1.1 above, we believe this to be the primary application intended by Congress in passing Section 9105 of the TBSSRA of 1988. The primary goal is to prevent the issuance of multiple licenses, with detection as a secondary goal, should the primary goal fail. Deterrence will follow from a reliable prevention or detection system.

A second application is the prevention, detection and deterrence of the use of a fraudulent commercial license by a driver. This application may also have been intended by Congress, as indicated by the transcripts of the hearings of the Subcommittee on Surface Transportation. Here, prevention of the issuance of genuine licenses, as duplicates or renewals, to drivers claiming fraudulent identities, is the primary goal. The manufacture and traffic in counterfeit licenses cannot be prevented by a biometric, or any other, system. However, a system designed to prosecute the secondary goal of detection of fraudulent use of licenses could be effective against fraudulent use of both genuine and counterfeit documents. Deterrence will follow from a reliable detection system.

In each application, prevention and detection require different system designs. A system to prevent the issuance of a multiple or fraudulent license will be implemented as an administrative function by the issuing agency. A system to detect the use of multiple or fraudulent licenses will be implemented as a law enforcement function and require a "roadside" component.

Consequently, there are four possible systems meeting the intent of Congress:

1) A system to prevent the issuance of multiple licenses to a single driver.
2) A system to prevent the issuance of a genuine license to a fraudulently identified driver.
3) A system to detect the use of a fraudulently obtained license.
4) A system to detect the use of multiple licenses by a single driver.

Additionally, a single system could be designed to meet some combination of these goals. Each system may require the development of different standards and each will have different costs and benefits.

4.2 Prevention of Issuance of Multiple Licenses

System alternative 1, to prevent the issuance of multiple licenses to a single commercial driver, is a "non-cooperative" application. Would-be violators are rewarded by the non-cooperative presentation of false measurements. For this reason, the biometric method chosen must be physiologically, as opposed to behaviorally, based. This ensures that, short of mutilation, a CDL applicant cannot willfully change his/her measure to avoid identification. Further, by the taxonomy of applications, use of the system will be in an "overt, non-habituated, supervised, standard environment."

The presented biometric measure is compared to all measures previously stored in a database of commercial drivers. Detection of a similar measure already in the database would indicate an attempt to obtain a multiple license. The scope of the system in this application will only be as wide as the access allowed to the stored biometric measures. That is, nationwide prevention of the issuance of multiple licenses would require the nationwide transmission of biometric measures. As will be discussed in Section 12, at least one state, Georgia, restricts the transmission of their driver's licensing biometric measures (fingerprints) beyond state borders.[20]

Regardless of the biometric technology chosen, the system would have the five functional elements discussed in Section 3: data collection, transmission, signal processing, storage and decision. For system alternative 1, the elements could be outlined as follows:

- Data Collection:
  - Record biometric identifier in the DMV upon application for a commercial driver's license.
  - Record other data.
- Transmission:
  - Transmit biometric data to state or federal centralized system with request for general search for matching biometric record.
- Signal Processing:
  - Extract feature vector.
  - Compare with database records at central location.
  - Send notification of any match to requesting DMV.
- Storage:
  - Store non-matched feature vector data in centralized database.
- Decision:
  - Deny license upon matching record.
  - Issue license upon finding of no matching record.

The storage system could be at the federal level or at the state level. Having the system at the federal or state level has significant implications. For instance, if the system were to be at the federal level, then standards for transmission and storage, which will enable a common storage and retrieval system usable for all states, will have to be used. Other issues, legal and political, related to the sharing of such information, will have to be addressed. Another form of a federal system may consist of having the data reside at the state level, but having communication and retrieval of information occur through a federal-level communications system. It should be noted that the issue of distributed computing, the extent to which computing occurs at centralized versus decentralized locations, could also be an issue. These issues of state versus federal centralized storage will be discussed in detail in Section 11 of this report.

This first alternative is a prerequisite to all other systems, and therefore, is considered as the minimum system implied by the legislative mandate of Section 9105 for standards development.

[20] Official Code of Georgia (Annotated) Section 40-5-2(c)(1.)(D) is discussed in greater detail in Section 12.3 of this report.

4.3 Prevention of the Issuance of Genuine License to Fraudulently Identified Driver

The second application, of preventing the issuance of a genuine license to a fraudulently identified driver, is a broader issue than can be addressed by a biometric system. AAMVA has developed a "best practices" list of acceptable identification source documents to address just this problem. No biometric system can establish a source identity for a new enrollee and no biometric system can protect against "collaborative" attacks involving licensing agency employees. A biometric system can, however, address the narrower problem of the issuance of single license to multiple drivers through a fraudulent renewal or duplicate application. In this scam, perpetrated in collusion with the legitimately licensed driver, a fraudster poses as the driver to gain a duplicate or renewal license with the fraudster's own photo image attached. A biometric system could prevent such fraud. Such a system is classified as "cooperative" and, as such, could be implemented using a variety of biometric technologies. Implementation of an effective system would be accomplished entirely on the state level, with no nationwide release of the biometric measure, by requiring that all applicants for a renewal or duplicate verify their identity in the issuing office by matching their current biometric measure with one previously stored. By the application taxonomy of Appendices A through C, use of the system will be in an "overt, non-habituated, supervised, standard environment."

This system, which we'll call system alternative 2, would work only in conjunction with the previous system. That is, system alternative 1 is a prerequisite for system alternative 2.

For system alternative 2, the functional elements could be outlined as follows:

- Data Collection:
  - Record biometric identifier in the DMV upon application for a renewal or duplicate commercial driver's license.
  - Record other data.
- Transmission:
  - Transmit biometric data and claimed identity to centralized system or system of issuing state with request to compare biometric data with record under claimed identity.
- Signal Processing:
  - Extract feature vector.
  - Compare with database record of claimed identity.
  - Send notification of match or non-match to requesting DMV.
- Storage:
  - No new data storage required but, depending upon biometric technology chosen, stored record could be updated.
- Decision:
  - Deny duplicate or renewal license upon non-matching record.
  - Issue license upon match with claimed record.

Given that system alternative 1 is a prerequisite for system alternative 2, the additional system components required are minimal. The major additional requirement is transmission bandwidth and system processing power. Consequently, including the functions of both alternatives 1 and 2 in a single system makes intuitive sense.

4.4 Detect the Use of Fraudulently Obtained License

While the first two system alternatives are administrative, with all components controlled by issuing agencies or some centralized administrative agency, the third and fourth are law-enforcement alternatives. These systems require "roadside" collection of biometric data from commercial drivers for comparison to data previously collected in an administrative setting.

The third application, that of detecting the use of a fraudulently obtained license, is classified as "cooperative, supervised, non-standard environment." The system might also be "habituated," depending upon the frequency with which any single driver was required to submit a biometric sample. "Fraudulently obtained" licenses would include both counterfeit licenses and genuine licenses fraudulently obtained as duplicates or renewals through identity misrepresentation. There could be two variations of such a detection system. One variation would compare a measure collected at "roadside" to the biometric record stored on the licensing document. Such a system would not be secure against professional counterfeiting unless the stored biometric was encrypted, such that the "roadside" verification systems each held the universal decryption key. Encryption would have to be by passing the enrollment biometric to a centralized agency. Only the centralized agency would hold the encryption key, as we cannot consider as secure any system with a distributed encryption capability, given the vulnerability of the entire system to theft or loss of a single encryption device.

This system would not require any data transmission capability from the "roadside" location. Devices for roadside biometric collection, card reading and verification are not currently available for any biometric technology, but could be easily developed commercially if a demand existed. However, use of the system nationally for "roadside" document verification would require a nationally centralized encryption capability and national standards for data storage on the license document.

National standards for data storage imply national standards for feature vector extraction, given the tremendous size of raw biometric measurement records. All current biometric methods use vendor-proprietary feature extraction techniques. We do not feel that a feature extraction standard for all vendors is possible in the near or intermediate future with any biometric technology. Consequently, we believe that this variation of the third application is not practically feasible.

A second variation in a system designed to detect the use of fraudulent licenses would compare the biometric measure collected at "roadside" to the biometric record stored in a centralized database. Such a system would require transmission of the claimed identity and the collected biometric record, perhaps processed at roadside, to the original licensing agency or to a centralized database. Encryption would not be necessary as no forgeable biometric data would be stored on the licensing document. Consequently, no national standards would be required for the licensing document. Standards would still be required identifying the biometric measure and the method of collection and transmission.

Both system variations assume that biometric identification has been collected and stored administratively during the license application process. For system alternative 3, the functional elements could be outlined as follows:

Variation 1:

- Data Collection:
  - Collect biometric identifier at roadside.
  - Read biometric identifier stored on the licensing document at roadside.
- Transmission
  - No data transmission required.
- Signal Processing
  - Extract feature vectors from collected biometric identifier at roadside.
  - Decrypt biometric identifier read from licensing document.
  - Compare the two records at roadside.
- Storage:
  - No new data storage required.
- Decision:
  - Detain driver upon non-matching records.
  - Permanent removal of the driver could only be through the judicial system.

Variation 2:

- Data Collection:
  - Collect biometric identifier and claimed identity at roadside.
- Transmission
  - Transmit the biometric data and claimed identity to the issuing agency or the centralized database.
- Signal Processing
  - Extract feature vector from collected biometric identifier at roadside or at the centralized location.
  - Compare the transmitted record with that stored under the claimed identity.
- Storage:
  - No new data storage required.
- Decision:
  - Detain driver upon notification from centralized or issuing agency of non-matching records.

  - Permanent removal of driver could only be through the judicial system.

4.5 Detect the Use of Multiple Licenses by a Single Driver

The fourth application, that of detecting the use of multiple licenses, is classified as simultaneously both "cooperative" and "non-cooperative." A biometric measurement collected at "roadside" would be transmitted to a centralized site for a search for multiple matches. It is cooperative in that, to defeat the system, the fraudster would have to match the license s/he was carrying. It is non-cooperative in that the fraudster would have to not match multiple records. Further, this system presumes the existence of a centralized data storage or communication site to direct the search against all stored biometric records.

For System 4, the functional elements could be outlined as follows:

- Data Collection:
  - Collect biometric measurement and claimed identity at roadside.
- Transmission:
  - Transmit biometric data with claimed identity to a centralized system with request for search against all stored records.
- Signal Processing:
  - Extract feature vector at centralized site.
  - Search entire database at centralized site.
  - Secondary comparison to record of claimed identity.
  - Send notification of all matches to requesting agent.
- Storage:
  - No new data storage required.
- Decision:
  - Detain driver upon notification of multiple matching records or non-match against claimed identity.
  - Permanent removal of the driver could only be through the judicial system.

Systems 3 and 4 require significant additions to the prerequisite system alternative 1. It is not at all obvious that an extension of system 1 to include these additional functions would be cost effective. This topic will be taken up in detail in Section 16.

5.0 A REVIEW OF THE MULTI-STATE STEERING COMMITTEE FUNCTIONAL REQUIREMENTS

On February 1 and 2, 1997, the AAMVA Biometrics Working Group met in Baltimore, Maryland, for the purpose of reviewing this project. Membership in the working group was established by AAMVA and included representatives from the states of Alabama, California, Indiana, Maryland and Texas as well as AAMVA and

AAMVANet. At this meeting, and in a subsequent meeting on September 22 and 23 in Sacramento, California, the functional requirements established by the "CDL Biometric Identifier Multi-State Steering Committee" were reviewed.

5.1 The Revised Functional Requirements

The revised requirements suggested by the working group are as follows, with additions shown in bold type:

> "1. The system will capture the biometric identifier from each applicant without increasing the net transaction processing time (the actual time a customer is in a DMV office) by more than 30 seconds.
>
> 2. The biometric identifier must be accurate, relatively unalterable, unique, physical characteristic that can be captured, recognized or verified and stored, and that is verifiable over an indefinite period of time.
>
> 3. The method of capturing the biometric identifier will be unobtrusive to the applicant. The method will be socially acceptable and will not endanger the health, safety, or welfare of any applicant.
>
> 4. The system of capturing, recognizing ~~or verifying~~ and storing each applicant's biometric record must have been previously tested for accuracy in an environment that proximates that of the CDLIS and with a less than ~~0.5% error rate~~ **10% false non-match error rate in the recognition mode. A recognition system false match should occur with no more frequency than one applicant in one million when the system is at the target enrollment level of 8.5 million.** ~~The error rate refers to both false accept and false reject errors~~. **In the verification mode, the false non-match rate should be less than 1% with a false match rate of also less than 1%.**
>
> 5. The system must be able to search and compare new biometric identifiers against stored records. The system must also be capable of performing verifications on previously established biometric records. The recognition process must be accomplished within 72 hours after receipt of the inquiry, and the verification processes must be accomplished with 5 seconds of receipt of the inquiry.
>
> 6. During the initial enrollment process (conversion) for previously licensed commercial drivers, the biometric data base file will grow from zero records to ~~5~~ **8.5** million records. Therefore, during the conversion, the system must be capable of searching and comparing the ~~5~~ **8.5** million current records and the 500,000 new CDL's issued each year against this growing data base. Once the biometric records on existing commercial drivers have been captured, compared and stored, the system must be

capable of annually recording, comparing and storing 500,000 new CDL applicants' biometric records. The system must also be capable of annually verifying the biometric records on ~~1.25~~ **2** million CDL renewal applicants, 250,000 interstate residency change applicants and 90,000 applicants seeking duplicate licenses and the anticipated ~~5%~~ **6%** a year growth in these types of applications.

7. The system must have a method of capturing, storing, and reporting management information, such as, the number of new biometric records accepted, the number of biometric records verified, the number of applicants the system was unable to "enroll," measurements of the quality of the information captured, system down time, the system errors by type, and average enrollment processing time on a daily, weekly and monthly basis.

~~8. The system must be compatible with and capable of interfacing with the CDLIS designed pursuant to the CMVSA.~~

9. The system must be reliable, allowing the states to provide uninterrupted service to their applicants.

10. Any biometric identifier capturing device must provide on-site, immediate identification of whether or not an acceptable biometric sample has been obtained, thereby guarding against the need for customers to make return visits to the local offices solely to recapture their biometric record.

11. The system must be simple to use. Use of the system must be easily understood by employees, and must be easy to explain to the states' customers whether they are English or non-English speaking.

12. In order to encourage maximum biometric system participation by the states, the system should offer sufficient flexibility in procurement options and the capture and transmission of the biometric data.

13. ~~The system must be capable of accurately accomplishing proper identification without a candidate list for 99.9% of the applications.~~ **The system must not require routine human intervention in the enrollment or matching processes.**

14. The system must be capable of interfacing with other biometric identifier systems using the same type of biometric and meeting standards for data exchange recognized by the American Association of Motor Vehicle Administrators (AAMVA) now or in the future for the biometric identifier captured. If the biometric identifiers is an automated fingerprint,

the interface must meet ~~NBS standards for Type I and Type II logical records~~. **ANSI/NIST fingerprint data format standards.**

~~15. Data template/minutiae must be capable of being incorporated on a data carrier card issued in the form of a driver's license.~~

~~16. The carrier must have the potential for remote verification when used with a data carrier license document."~~

5.2 AAMVA Functional Requirements and System Applications

In comparing the AAMVA revised functional requirements to the system functions of Section 4, it is clear that the AAMVA functional requirements encompass both system alternatives 1 and 2. Functional requirements 15 and 16 were dropped from the original list by the AAMVA biometrics working group because of concern over the political difficulties of template standards development. This implies that the detection capabilities of system alternatives 3 and 4 of Section 4 above are no longer AAMVA functional requirements, but can be considered as additional system options.

6.0 CRITERIA FOR TECHNOLOGY SELECTION

Fundamental to the selection of candidate technologies was the creation of a reasonable criteria for selection. Because of the potential size and public profile of a large-scale project for the biometric identification of commercial drivers, we can expect some segments of the biometric industry to take issue with any narrowing of the candidate technologies. Consequently, we put considerable care into establishing a fair and rational set of criteria. Appendices A through C were written to establish our basic approach. The Functional Requirements alone are insufficient to narrow the field of potential technologies as most vendors would claim their ability to meet these requirements even at large-scale. Additional independent, large-scale testing to substantiate vendor claims is not possible, so tighter criteria were developed.

We have determined that any candidate technology should:

1) be claimed by vendors to support at least the application taxonomies of system alternatives 1 and 2.
2) have been used previously in a large-scale application of the same taxonomies for which an independent performance/cost audit is available indicating that the revised functional requirements can be met.
3) be available from multiple vendors supporting a single image collection, compression and storage standard.

Criterion 1 is important as it allows a tremendous narrowing of the candidate technologies to those which are claimed to support both the "non-cooperative" and "cooperative" applications of system alternatives 1 and 2. It must be understood that meeting this criterion is necessary, but not, by itself, sufficient in the technology selection process. "Non-cooperative" applications require physiologically-based, as opposed to behaviorially-based biometric methods. Of the physiologically-based technologies, only retinal scanning, fingerprinting and facial imaging vendors claim to support both non-cooperative and cooperative applications.[21]

Criterion 2, implicit within Functional Requirement 4, allows us to limit the risk to the agencies implementing the project by requiring some previous, audited demonstration of the technology at large-scale. The scalability of any technology from small-scale or laboratory demonstration to large-scale implementation is a question not easily resolved by theoretical calculation alone. This is due to both uncertainty in the scaling of hardware to achieve the required throughput rate, and to uncertainty in the capability of the algorithms to attain the required miniscule false match rates. Only fingerprinting has been used in large-scale non-cooperative applications. Independent performance results and cost data are available. As of this report, the largest civilian non-cooperative biometric system of which we are aware is the Automatic Fingerprint Identification System (AFIS) in use by the State of New York Department of Social Services. It has approximately 950,000 enrolled persons in the database. We feel comfortable in extrapolating this performance to the 8.5 million size required for the commercial driver system.

Criterion 3 is required by Functional Requirement 12 of Section 5 to "offer sufficient flexibility in procurement options and the capture and transmission of the biometric data." Only fingerprinting and facial imaging is available from multiple vendors supporting a single image collection, compression and storage standard.

On this basis, we believe that only fingerprinting can currently meet the three criteria above for all of the system functions discussed in Section 5 of this report. We do not believe that any other technology will meet these criteria within the next five to ten years. Based on the analysis methodology and data of Appendices D, E and F, and a review of several extant AFIS, including the Los Angeles County Department of Social Services AFIRM system, the California Department of Justice AFIS, and the State of Texas Department of Public Safety driver's licensing system, we believe that an AFIS based on currently available technology could be designed to approximately meet all of the revised functional requirements of Section 5.

Current AFIS systems are computationally the fastest of all existing biometric systems. There is no computational or accuracy advantage to be accrued by adding additional biometric identifiers, beyond additional fingerprints, to each individual record.

[21] While it is our opinion that iris scanning could, in theory, support non-cooperative applications, the current design was intended for cooperative applications such as access control, according to public declarations by IriScan. One voice recognition system vendor claims to support non-cooperative applications, but informal testing has not supported that claim.

7.0 HOW CIVILIAN FINGERPRINTING SYSTEMS WORK

All automatic identification systems, including AFIS, can be "modularized," at least conceptually, into components as illustrated in Figure 1 of Section 3. We emphasize that Figure 1 is intended to be as general as possible, meaning that actual systems may vary somewhat from the system illustrated. The sub-systems are data collection, transmission, signal processing, storage and decision. The purpose of this section is to review Figure 1 in specific application to fingerprinting systems.

7.1 The Data Collection Sub-System

Figure 1 illustrates the process in which a biometric pattern, which in our case is a fingerprint, is presented to a sensor and converted into a digital electrical[22] signal. The fingerprint varies physiologically between collection sessions, depending upon skin damage and dryness. The "presentation" of the fingerprint, that is the pressure, angle, and rotation of the finger on the sensor, may also vary.

The scanner, operating with a "frame grabber," creates a digital image of the fingerprint. In all non-cooperative systems, the use of the scanner by the customer is supervised by a system attendant. In our classification scheme, non-cooperative AFIS systems are always "attended." It is the purpose of the attendant to assure that the presentation is adequate to result in a processable print and that the correct finger is placed by the customer on the device. The attendant must assure that the "core" of the fingerprint (the central area) is centered on the scanner.

There are two basic styles of scanner (usually called "flat" and "live", although terminology varies) with multiple technological implementations. A "flat" (also called "planar") scanner captures an image of the flat part of the finger around the core, pressed statically against a transparent "platen." A "live" scanner captures an image rolled onto the platen which includes skin areas on the sides of the finger. "Live" scanners are used for ten-print, FBI standards-compliant, forensic applications. "Flat" scanners are used for civilian applications such as screening for social service benefits and facility access control. These scanners are manufactured by over a dozen vendors, giving the states procurement options.

The standard technology for either of these scanners uses a "charge coupled device" (CCD) camera which is fed an optical image through mirrors and lenses. A focal length of several inches is required for most of these cameras, causing the scanners to generally be several inches in length and width. A finger placed on the platen results in the "frustrated internal reflection" of the light along the ridges and complete reflection at the valleys. The resulting gray-scale image is dark along the ridges and light along the valleys.

Optical scanners are subject to performance degradation as focal paths get out of alignment and as the "platen" becomes worn and scratched. Dryness or exposure of the

[22] Holographic systems modulate fingerprint images onto light signals, so are exceptions to this rule.

skin to chemical or mechanical abrasion prevents the clear imaging of the finger. Several vendors make skin moisturizing compounds that can be helpful in obtaining clearer images.

A "frame grabber," either internal to the scanner or placed inside the computer, converts the optical image into a digital representation, using at least 8 bits (256 levels of gray-scale). Frame grabbers frequently add noise and distortion to the fingerprint image.

Several competing technologies have been introduced over the last 2 years into the flat scan market. One technology uses ultra-sound to acoustically image the finger. This acoustic scanner is commercially available, but there are, at this writing, no large-scale installations using these devices.

Three companies have prototyped and privately demonstrated solid-state, flat "scanners on a chip." Each of these scanners uses a different technology: electrical conduction, capacitance, or thermal energy. None of the chip technologies is commercially available as of this writing.

The FBI has established image quality standards[23] for "live" scan devices for forensic applications and will "certify" scanners as meeting this standard. The standards set minimum signal-to-noise ratio, minimum pixel resolution, bounds for "modulation transfer function" (a smearing distortion measure), minimum image contrast measures, and maximum x-y coordinate distortion. The standard fails to set minimum size requirements, however, for the fingerprint images. Neither the FBI nor any other group has established standards for non-forensic, flat scanners, which sell at prices half those of the FBI-compliant "live" scanners.

Images from FBI compliant scanners have roughly 400 x 400 pixels, each pixel containing 8 bits (one byte) of gray-scale information. This computes to an image size of approximately 160 kbytes. If the image is to be placed into a standardized format (such as a "bit map" or a "TIFF" file), additional bytes are required for header information.

7.2 The Transmission Sub-System

The transmission sub-system may operate with signal compression prior to transmission and signal re-expansion prior to signal processing.

7.2.1 Signal Compression

As mentioned, images from the scanner require roughly 160 kybtes. To reduce storage and transmission bandwidth requirements, it is standard to compress images. The compressed images can be transmitted or stored, then re-expanded for viewing or feature extraction. Most compression methods have variable "compression ratios." The greater

[23] "Appendix G: Interim IAFIS Image Quality Specifications for Scanners," CJIS-RS-0010(v4), 1995, included in this report as Appendix G.

the compression ratio, the smaller the compressed data file. A 20-to-1 compression ratio, for instance, reduces a 160 kbyte image to 8 kbytes.

In all data compression applications, there are two families of compression procedures: "loss-less" and "lossy." A "loss-less" procedure produces an image after compression and re-expansion that is exactly the same as the original image. A "lossy" procedure produces reconstructed images that differ, at least mathematically but perhaps not perceptually, from the original. The amount of information loss increases with the compression ratio, so there is a trade-off between image reduction and information loss.

Until 1993, fingerprint images were generally compressed using a "lossy" image compression method known as JPEG.[24] This method was designed to provide 20-to-1 compression rates on natural scenes (photographs and the like) in such a way that the compression losses would be scarcely perceptible to the human viewer. The JPEG method arbitrarily divides an image into blocks, then seeks the coefficients of a mathematical equation (the discrete cosine transform) that best fits the image in each block. Problems occur with JPEG at the block boundaries, where the image becomes discontinuous. This has the unfortunate effect with fingerprints of creating the false appearance of ridge minutiae. Lacking any other standardized compression method, however, AFIS fielded before 1993 used JPEG for the storage and transmission of fingerprints.

In 1993, the FBI created the "Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification"[25] for the compression of fingerprint images. Like JPEG, WSQ is a "lossy" method based on extracting coefficients of a mathematical representation of the image (based on a wavelet transform[26]) and is capable of 20-to-1, or higher, compression. Unlike JPEG, however, WSQ was specifically designed for the compression of fingerprints with the minimum loss of ridge and skin pore data. The WSQ algorithm does not divide the image into blocks and, therefore, does not create image discontinuities at block boundaries as with JPEG. Although WSQ can be performed at variable compression ratios between 1 and at least 50, the FBI established 15-to-1 as the standard WSQ compression ratio based on subjective testing with human fingerprint experts. It is rumored that the chosen compression ratio would have been higher but for the objections of the "latent[27]" print examiners. The extent to which WSQ compression ratio affects AFIS error rates is not known. WSQ is now firmly established as the international "de facto" standard for fingerprint image compression and is supported by all major AFIS vendors.

[24] So named for the "Joint Photographic Experts Group" which created the standard.

[25] Criminal Justice Information Services, Federal Bureau of Investigation, IAFIS-IC-0110v2, February 16, 1993.

[26] The term "wavelet transform" refers to a generic method of modeling data. The specific nature of the transform depends upon the "mother wavelet" chosen. For WSQ, a five-coefficient wavelet was specifically designed to best match fingerprint patterns.

[27] Latent prints are those left behind on materials and "lifted" by forensic examiners. They prints may be of extremely poor quality and may not contain the core of the fingerprint and are, therefore, the hardest prints to match.

7.2.2 Data Transmission Format

Proper understanding of a transmitted image requires that information about the data format, form of compression, and image source be included with the image itself. NIST and the FBI have released a standard data format for fingerprint images. That document, "Data Format for the Interchange of Fingerprint Information," ANSI/NIST-CSL-1-1993, is included in this report as Appendix I.

7.3 Signal Processing Subsystem

The signal processing subsystem has several components, including feature extraction, quality control and pattern matching.

7.3.1 The Feature Extraction Module

The digital image captured by the scanner and digitized by the frame grabber is too large to deal with effectively, particularly as it must be compared with a database of other, similarly sized images. Further, the raw image may contain presentation- and sensor-dependent information extraneous to the process of fingerprint matching. For the purposes of efficient and accurate image matching, each fingerprint must be reduced to a small set of important "features." Non-essential features, such as scars and cracks, and image translation and rotation, are discarded. In general, this process is non-reversible, meaning that the original fingerprint cannot be reconstructed from the extracted features. What these features represent depends upon the feature extraction method used, of which there are three: correlation, transform, and minutiae.

Correlation methods find a small number (say, 5) of small areas of the image deemed in some way to be "interesting" (high ridge density or flow field variation, for instance). The x-y position of these small areas, as well as the fingerprint pattern inside those areas, are the "features" to be passed to the pattern matching algorithm.

Transform methods rely on arcane mathematical techniques. A mathematical equation capable of representing any fingerprint is arbitrarily chosen. Then, for each fingerprint image, the equation coefficients are chosen so as to represent (or model) the image as well as possible. Some of these coefficients may have very small values, allowing them to be discarded without the loss of excessive information about the details of the fingerprint. The remaining coefficients are considered as the feature vector and are passed to the pattern matching algorithm.

All of the large-scale AFIS vendors with whom we are acquainted use a "minutiae-based" approach. Minutiae methods are modeled after the techniques that have historically[28] been used for the identification of fingerprints by human experts. The goal is to locate and extract the ridge endings and bifurcations (minutiae) present in nearly all

[28] Minutiea methods were first discussed in Francis Galton, "Personal Identification and Description," *Nature*, June 21, 1888, pp 173-202

fingerprints.[29] The minutiae extraction process begins with compressing the ridges to a width of one pixel, then converting the gray scale into pure black and white. A "skeletonized" image results. Most minutiae extraction algorithms then attempt to "heal" the ridges: filling them in where scars or imaging problems have caused the appearance of false ridge endings. Now, having a "healed" skeleton, the algorithm goes searching for ridge endings and bifurcations (splits). The location of these minutiae are, perhaps, recorded and passed on to the pattern matching algorithm.

These features, no matter from which method extracted, are the most compressed representation of the fingerprint to be had in any system. In large-scale systems, these representations are generally 512 or 1024 bytes in length, depending upon vendor. Consequently, it is the "feature vector," or a smaller version (100 to 256 bytes), that is stored on driver's licenses and identification cards for later use in cooperative applications for verifying the identity of card holders. These feature vectors are also stored in the database for use in matching to sample features from new customers. Stored feature vectors are referred to as "templates" and are taken as the "true" identifier of the enrolled customer.

All feature extraction methods are proprietary. This implies that features from one company can only be read and interpreted from equipment supplied by that company. Further, as the original image cannot be reconstructed from the features, feature sets from one vendor cannot be translated into features of another vendor. If such features were to be used on licensing documents, as originally suggested by the Multi-State Steering Committee but removed in the revised functional requirements, cards produced by one vendor could not be read by equipment from another and all cards would require replacement if the vendor were to be changed. Features in a database could not be translated if the system vendor were to be changed during the life-cycle of an AFIS, meaning that a change in vendor would require re-enrollment of all persons represented in the database.

Further, we would expect there to be differences in the false match and non-match error rates based on feature size and characteristics. There is no data available on system performance as a function of the details of stored features.

One fingerprint system vendor, Printrak, is promoting "open architecture" and has offered to make their feature extraction method public. There has been little public response to this offer from the industry.

7.3.2 The Pattern Classification Module

Although not shown in Figure 1, a unique feature of large-scale AFIS is the addition of the pattern classification function to the feature extraction module. The

[29] Rumors persist that minutiae-less prints (a theoretical possibility) have been observed. Such prints would have perfectly continuous ridges, with no ridge endings or splits. These observations have never, to our knowledge, been verified. We have observed, however, fingerprints that, through injury or disease, do not display ridges in the usual sense, but rather consist entirely of bumps or scar patterns.

purpose of pattern classification is to allow the "binning" of fingerprints during the matching process. In large-scale systems, it is computationally inefficient to match features of each input print against the stored features of all enrolled prints. Some stored prints can be eliminated from comparison on the basis of differences in pattern classification. For instance, many civilian AFIS use a classification system very close to that originally proposed by Galton[30], based on arches, left loops, right loops, and whorls, but there are other approaches as well. Some vendors simultaneously use multiple binning techniques, as explained in Appendix E.

Many prints are difficult to clearly classify and are given multiple classifications or designated as "unknown." Input prints are matched only against stored prints that have been given at least one of the same classifications or designated as "unknown"[31]. Consequently, input prints require matching against only a portion of the stored database. This portion, expressed as a percentage, is known as the "penetration rate." The lower this "penetration rate," the fewer comparisons will be expected and the more efficient the system.

If the system uses multiple fingers, it is possible to bin each finger according to the classifications of the fingerprint ensemble. In other words, if two prints are taken from a customer, the first being of classification A and the second of classification B, each print can be binned according to the classification of the two print combination, AB. The sample first print will be compared only to first prints in the database from people whose ensemble classification was also AB, although unknowns must also be considered. This allows for a multiplicative decrease in penetration rate for multiple print systems.

There is a cost in terms of error to be paid for this increase in matching efficiency, however. If a sample print is placed in a different bin than a truly matching print in the database, the two prints will never be compared and a false non-match will result. The probability that a print will be inconsistently binned is known as the "bin error rate."

At this point we should mention fingerprint "filtering," often confused with "binning" because its goals are the same. "Filtering" involves additional partitioning of the database based on information, such as gender or age of the customer, which is not contained in the fingerprint image itself. Identification of the finger ("right thumb," for instance) cannot be made based on the fingerprint pattern[32], so the partitioning of the database by finger, as done in all AFIS, is a filtering process. Because filtering is based on exogenous information, it is not part of the signal processing process, but rather, is part of the data collection process accompanying the sampling of the customers. Flow of this information is not shown in Figure 1.

[30] Francis Galton, Fingerprints, (London, McMillan, 1892)

[31] The binning procedure described here is "hard," meaning that only the single bin is searched and if a matching print is not found the search is stopped. Some vendors have "soft" procedures, allowing neighboring bins to be searched in the event that no match is found in the primary bin. All systems studied have a provision by which the operator can over-ride the filtering procedure, allowing all bins to be searched if there is any ambiguity in the source (gender of applicant or presented hand) of a particular print.

[32] At least one company is working on an algorithm that would differentiate left and right index fingers reliably. If implemented, the "left-right" filtering would become "binning" in our terminology.

Filtering also results in errors, but these errors are those made by the human operators of the system, perhaps encouraged by deceptive activities of customers attempting fraud, and cannot be estimated by engineering tests. In other words, filtering leads to search efficiencies while externalizing the associated errors, so consequently is greatly appreciated by AFIS vendors. At the same time, the presence of filtering creates vulnerabilities exploitable by those not wishing recognition by the system.

7.3.3 The Quality Control Module

Because of imaging problems caused by the factors discussed in the scanner section of this report, the captured fingerprint might not be readable. All AFIS vendors have some sort of "front end" quality control allowing the system attendant to verify the quality of the fingerprint image while the customer's finger is on the platen. Quality control modules make "accept/no accept" decisions based on some or all of the following criteria:

1) Gray scale contrast.
2) Connectivity of the ridges.
3) Number and extractability of features from the images.

An additional problem in obtaining usable images from any type of scanner is assuring the consistent placement of the finger on the platen. Variations in finger placement can leading to a readable, but not repeatable, image. The most straight-forward way of assuring repeatability is to require the presence of the fingerprint core in the image. We know of no current quality control software capable of detecting the presence of the core, although the major AFIS vendors are actively developing software to do so.

Figure 1 shows quality control after feature extraction, but this is not always the case. Depending upon the criteria used, quality control can be done before or after feature extraction.

There are no standards regarding quality control modules in fingerprinting systems. Some modules will assist the customer in proper finger placement, making recommendations as to finger movement so as to correctly capture the fingerprint core. Some quality control modules have user selectable sensitivities affecting how readable a print must be to be accepted by the system. Some modules rate the fingerprints as to being "A," "B" or "C" quality. There are no standards regarding the rating of fingerprint images and there is no data relating AFIS performance to image quality. The Multi-State Steering Committee's Functional Requirement number 10 requires some front end quality control. This requirement can be met by all major AFIS vendors.

Civilian AFIS generally transmit the images to the signal processing subsystem
l perform the signal processing in "real time," meaning while the customer is still at
image scanning device. After the extraction of the features, the sample is checked for

"quality," generally related to the number of minutiae extractable from areas of the print where the ridge structure is coherent. If the quality is deemed insufficient, the system operator is instructed to collect a replacement sample from the customer. When the quality of the received image is deemed sufficient, or when overridden by the system operator in the case of difficult prints, the extracted minutiae features are sent to the matching module.

7.3.4 The Pattern Matcher

The purpose of the pattern matcher is to determine a similarity score between the presented sample and the stored templates in the database or on the identification card. If the score is larger than some arbitrary threshold, a "match" is declared.[33] If smaller, a "non-match" is declared. It is clear that the chances of a match or non-match are dependent upon the chosen threshold. As the threshold is decreased, there is a trade-off between a decrease in false non-matches and an increase in false matches. The threshold is adjusted either by the vendor or the system administrator to implement the policy with regard to error rates.

The precise method used to measure the similarity between sample and template depends upon the features being used. Transform methods use "euclidean"[34] distances familiar to students of geometry. Correlation methods generally use geometrically-based distance measures, as well, although they may not be strictly "euclidean." Minutiae methods use arcane similarity measures that are extremely hard to characterize mathematically. All similarity measures vary from vendor to vendor, with minutiae-based measures varying in the extreme.

During enrollment, each customer's fingerprint pattern is searched against the database to ascertain that the customer is not previously enrolled. To save search time, however, "binning" and "filtering" is used to divide or "partition" the database into smaller sections, as discussed in preceding sections. The database in structured by the various partitions and the sample print is searched only against prints in the appropriate partition

All multiple print systems studied by us search the database against two prints. If a match is found for either print, the customer is declared to be previously enrolled in the database. Because this may imply criminal fraud on the part of the customer, the data, both samples and matching templates, are sent to a "trained"[35] operator for verification and a recommendation regarding handling of the potential criminal case.

[33] In this regard, minutiae-based fingerprinting is different from other biometric methods that use distance measures in place of "similarity" scores. Opposite to the similarity scores, the distance measure decreases with increasing similarity of the compared images.

[34] A euclidean distance is computed by the Pythagorean theorem: the square of the distance between two points being equal to the sum of the squares of the distances between points in each coordinate direction.

[35] In the LA AFIRM system, training consists of a several-week course given by the system integrator to three or four staff employees.

7.4 Storage Sub-system

The storage sub-system contains two kinds of data: the extracted features and the fingerprint images.

7.4.1 Feature Storage

As mentioned, it is the features, being the most compressed representation of the fingerprint, that are stored on driver's licenses and identification cards for later use in verifying the identity of card holders. The features are also stored in the database for use by the search algorithm when matching new samples. Assuming 1 kbyte minutiae records, a two-print system with 8.5 million enrolled persons would require a mere 17 gigabytes of feature storage.

7.4.2 Image Storage

Because fingerprint images are required for legal proceedings and in the event that the feature extraction system is changed (perhaps owing to a change in vendors during the life of the system), it is necessary to store and preserve compressed fingerprint images. Assuming 15-to-1 compression on 160 kbyte images, each image will require approximately 15 kbytes of storage, if header information is included. In a fully deployed 8.5 million person two-print system, this will require around 250 gigabytes of storage, which is a fraction of what is currently available in large AFIS installations.

7.5 The Decision Sub-System

It is the function of the decision sub-system to determine if a "match" has been found based on some decision policy established by the system user (not the vendor). The policy may be to declare a "match" if the similarity measure is above some threshold, or if the sum of two consecutive measurements is above some threshold, or under any of a set of conditions limited only by the imagination of the designers. The system policy may be to "accept" a customer for enrollment if no match is found over some number of presented fingers and to "reject" a customer for enrollment if matches are found on some number of fingers. The system might also "accept" a customer for renewal if a match is found against some number of claimed prints and "reject" a customer for renewal if no match is found. In any case, the precise decision policy is a question to be worked out during implementation by the system user and will vary according to the functions the system is required to perform and the allowable error rates.

7.6 Field Verification Systems

A verification system differs from an enrollment system only in that its sole purpose is to match the presented biometric sample to a single, previously stored template, thus identifying the customer as the one previously enrolled. The previously stored template might be available from a database over a communication line or from a card presented by the driver in a "roadside" application. Feature extraction and quality control are still needed, as is the capacity to make a single similarity measurement (between the sample and the stored template) and a decision based on a threshold. No storage of the new sample or of the sample features is required. Consequently, verification systems could be made significantly smaller, cheaper and even portable. We have seen vendor prototypes of small hand-held field systems, but, as of the date of this report, have not seen such a system demonstrated or marketed.

8.0 THE PROBLEMS WITH FINGERPRINTING

The wide acceptance of fingerprinting in forensic applications has lead to an overly optimistic view of the attainable accuracy of AFIS systems. This is both good and bad: good in the sense that the public perception of high accuracy and correct match rates serve as a powerful deterrent to fraud; bad in the sense that these perceptions by system operators and administrators can lead to over-confidence in the system and subsequent laxness in ancillary fraud prevention procedures. In "non-cooperative" applications, such as the system of our primary focus, operational false match rates are easily measured in that a false match, resulting in the incorrect denial of a license application, is always reported. False non-match rates cannot be measured in this application because they can only result from a fraudulent multiple enrollment and will never be reported.

In our CDL system, a false non-match will result in the issuance of a multiple commercial driver's license document. The number of fraudulent multiple license issuances is equal to the product of the fraud rate and the false issuance rate. The continued perception of system accuracy by the customers will drive down the fraud rate to the point that the number of fraudulent issuances is minuscule. So what is most important here is the continued perception of a low false non-match rate, more than the actual rate itself. The relationship between the true non-match rate and the fraud rate is not known, but we can speculate that the 1% false non-match rate required by the revised functional requirement 4 of Section 5.1 is far lower than necessary to discourage would-be fraudsters

In this section, we will discuss the factors contributing to a false non-match rate that, in practice, may grossly exceed benchmark test error rates based solely on algorithm failures.

A few of these factors are:
1) Deceptive Practices by the Customer.
3) Bad prints, missing fingers.
4) Lack of adherence to, and inadequacy of, the standards.

8.1 Deceptive Practices by the Customer

There are a number of deceptive techniques that could lead to a false issuance of a multiple driver's license document if employed by a customer. For security reasons, not all of these will be discussed in this report.

The easiest deception is to defeat any of the filtering methods, such as by gender or age impersonation. Consequently, the filtering approaches used, if any, should not be publicly disclosed. Finger identification is based on external data and is, therefore, a filtering technique. Any replacement of a left forefinger for a right, or a middle finger for a forefinger, for example, will defeat the system. Vigilance by the system operators is the only countermeasure for attacks on the filtering methods.

Fingertip mutilation is a crude, but well-known approach. Caustic chemicals can cause the temporary destruction of the ridge patterns. Such attacks can be revealed by the front-end quality control software. The only countermeasure for such attacks is to require persons with damaged fingers to return at a later date for enrollment.

Less effective and more obvious techniques include coating the finger with nail polish or superglue. Such blatant attacks, when revealed by the quality control software and noted by the system operator, could be dealt with using on-site administrative actions.

8.2 Bad Prints and Missing Fingers

At any particular time, some percentage of the population cannot give good fingerprints under even the best conditions, including the use of special moisturizing compounds. From data collected in the Philippine AFIS Benchmark Study, we estimate this percentage to exceed 3%. The causes are multiple: missing hands or fingers; chronic skin infections; chemical exposure; mechanical abrasion. Cement and brick workers, guitarists and house cleaners are believed to be particularly likely to have unreadable fingerprints. Fingerprints from such people can be extremely cracked and "non-minutiae based." Some images of damaged prints follow as Figure 2..

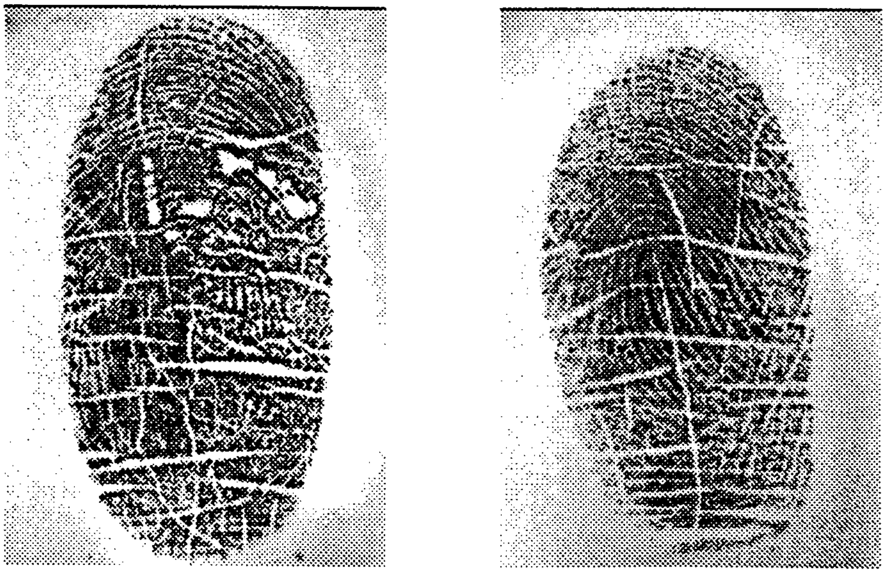

FIGURE 2: DAMAGED FINGERPRINTS

8.3 Adherence to Standards

Even the most physiologically beautiful fingerprints will not be matchable if adequate standards are not used in collection, compression and storage. As explained in Section 3, repeatability of biometric measures depends not only on the physiological quality, but also on consistency of presentation and sensor quality, and on the errors introduced through compression. The California Department of Motor Vehicles has been collecting thumb prints from all driver's license applicants for over a decade. At the time that the California system was implemented, quality control software was not generally available. California now estimates that less than 60% of all the prints collected are readable due to sensor and presentation degradation. Even today, there are no standards for presentation quality, meaning that a system meeting all sensor, compression and transmission standards might still produce unreadable or unmatchable images.

Further, as previously mentioned, “legacy” systems using JPEG compression have noted artifacts within the re-expanded images. These systems may also store images in proprietary formats not readily accessible with current software. Consequently, adherence to technical standards for sensor quality, compression and data format is necessary, but not alone sufficient, to assure required system accuracy levels.

9. 0 PREDICTING AFIS PERFORMANCE IN APPLICATION TO COMMERCIAL DRIVERS

Detailed mathematical models for AFIS performance prediction are presented in Appendices E and F, "Large-Scale Civilian Biometric Systems – Issues and Feasibility" and "Error Rate Equations for the General Biometric System." Appendix E also includes results of the Republic of the Philippines Civilian AFIS Benchmark Test, which provides the parameter values needed to predict AFIS performance at large-scale. This section will summarize these findings.

9.1 System Parameters

There are five important, non-independent parameters that govern the performance of Automatic Fingerprint Identification Systems. These are: 1) the "penetration rate," reflecting the expected percentage of the fingerprint database to be compared to a sample print; 2) the "bin error rate," or probability that a search for a print in the database will be unsuccessful because the sample and template prints were placed in differemt "bins"; 3) the single comparison false match rate, or probability that two non-matching prints will be incorrectly matched; 4) the single comparison false non-match rate, or probability that two matching prints will be incorrectly not matched when compared; 5) the "one-to-one," or "cold match" comparison rate of the hardware.

9.2 Penetration Rate

The system penetration rate reflects the matching efficiencies achieved by placing the database fingerprints into "bins" based on classification type, ridge count or some other measure endogenous to the fingerprint itself, and gains based on exogenous "filtering" techniques, including identification of the finger in multiple finger systems and identification of the customer's gender. Generally, a single print can be placed into multiple bins or filter partitions if there is uncertainty regarding its classification. Some prints of extreme uncertainty as to classification are labeled as "unknown" and placed in all of the partitions. In operation, a sample print is classified according to the same system as the database, then matched against only those prints from the database which are in the same classification or classifications. The average, or expected, percentage of prints to be matched for each input sample is the "penetration rate." Of course, the smaller the penetration rate, the more efficient the system.

Binning and filtering are generally independent operations and can be considered separately. In multiple fingerprint systems, system penetration rate is a function of the binning of the single fingers. This binning is not statistically independent, meaning that if the left thumb is a loop, for instance, the right thumb is likely to be a loop. Correlations between finger binnings are currently not widely known, so in developing our equations, we make the incorrect assumptions that the binnings are statistically independent between fingers and the same for all fingers. As possible, we will point out the direction, although not the magnitude, of the error this causes. Under these incorrect assumptions in an M-finger system, the multiple finger penetration rate, P_{mf}, can be written as

$$P_{mf} = P_{sf}^{M} \tag{1}$$

where P_{sf} is the single finger penetration rate. We note that penetration rate decreases geometrically with M. Correlations between finger binning actually causes this penetration rate to be higher (worse) than calculated using this equation.

Providing that filters are independent, as is generally the case, filtering factors are similarly multiplicatively combined, where the system filter factor, F, can be calculated from each individual filter factor, Fi, as

$$F = \sum_{all\ filters} F_i \tag{2}$$

The system penetration rate, P_{sys}, is the product of the bin penetration rate and the filter factor

$$P_{SYS} = P_{MF} * F \tag{3}$$

9.3 Bin Error Rate

The bin error rate reflects the percentage of prints falsely not matched because of inconsistencies in the binning process. Filtering errors, made by human operators during the customer interview process, occur outside of the "automatic" boundaries of the Automatic Fingerprint Identification System, so are not considered within the AFIS. In a multiple print system using ensemble binning, to not make a bin error requires that no bin error be made for any print. This awkward English actually best describes the underlying probabilistic relationship

$$1 - \varepsilon_{bin\,ensemble} = (1 - \varepsilon_{sfbin})^{M} \quad . \tag{4}$$

where $\varepsilon_{\text{bin ensemble}}$ is the system bin error rate, $\varepsilon_{\text{sfbin}}$ is the single finger bin error rate, and M is the number of fingers in the ensemble. Equation (4) assumes that bin errors are independent between fingers. This might not be true if the extent of finger damage is related between fingers. If damage is related, the true system error rate would be lower.

Equation (4) can be rewritten as

$$\varepsilon_{bin\,ensemble} = M * \varepsilon_{sfbin} - O(\varepsilon^{2}_{sfbin}) \tag{5}$$

where $O(\varepsilon^2_{\text{sfbin}})$ indicates terms of order $\varepsilon^2_{\text{sfbin}}$. For small $\varepsilon_{\text{sfbin}}$, as is the general case, (5) reduces to

$$\varepsilon_{bin\ ensemble} \approx M * \varepsilon_{sfbin} \tag{6}$$

We saw in the above section that penetration rate decreased exponentially with M. Here we see that system bin error rate increases multiplicatively with M. This indicates the general operational tradeoff between decreasing penetration rate and increasing bin error rate. This same relationship holds with increasing number of bins, K, for which $p_j \neq 0$: Penetration rate decreases while bin error rate increases.

9.4 Single Comparison False Match Rate

A single comparison false match occurs when a sample print is incorrectly matched to a print in the database by the decision subsystem because the similarity score between the two exceeded a fixed threshold. The "impostor" probability distribution function, $\Psi_I(s)$, is a function of the positive similarity measure s, which increases with increasing similarity between compared prints. Unlike other biometric systems, the impostor distribution function is closer to the origin (s=0) on the abscissa than the "genuine" distribution of similarity scores between truly matching prints.

The single comparison false match rate can be expressed as a function of decision threshold, τ, as

$$FMR(\tau) = \int_{\tau}^{\infty} \Psi_I(s)ds = 1 - \int_{0}^{\tau} \Psi_I(s)ds \tag{7}$$

which decreases with increasing decision threshold.

9.5 Single Comparison False Non-Match Rate

A single comparison false non-match occurs when a sample print is incorrectly not matched to a print from the same finger by the decision subsystem because the similarity score between the two is less than a fixed threshold. The single comparison false non-match rate, FNMR, can be given as a function of decision threshold, τ, as

$$FNMR(\tau) = \int_{0}^{\tau} \Psi_G(s)ds \tag{8}$$

where $\Psi_G(s)$ is the genuine probability distribution function. FNMR increases with increasing decision threshold. It is clear from equations (7) and (8) that false match and false non-match rate are competing factors based on the threshold.

9.6 Single Comparison Match Rate and System Throughput

The single comparison match rate is the number of "one-to-one" comparisons per second that can be made by the hardware of a single sample print to templates retrieved from the database. It is a function of the hardware processing speed, the template size, and the efficiency of the matching algorithm. AFIS system architecture is modular in the sense that processing speed can be designed to meet seemingly any requirement, although there are, no doubt, limits of scale as speed requirements get too great. As a rule of thumb, hardware costs run several US$ per match per second.

An approximation for the system throughput rate, T, depends upon: the comparison rate, C; the system penetration rate, P_{sys}; the number of records in the database, N; and the number of fingers to be matched, m. We have given the lower case symbol, m, to the fingers to be matched to differentiate it from the previously used, M, the number of fingers collected, upon which ensemble binning is performed. In all cases,

$$m \le M$$

In multi-finger system, initial search can be done on a subset, m, of the collected fingers, M. Any matches determined for any finger can be verified against the remaining M - m fingers. Under the assumption that no matches will be found, the throughput rate can be written as

$$T = \frac{C}{P_{sys} * N * m} \tag{9}$$

Violations of our assumptions regarding finger binning independence increase penetration rate and decrease throughput. Any matches found (false or correct) require additional M - m comparisons, further decreasing throughput, so this equation is an optimistic upper bound.

This throughput rate must match the customer input rate, I, as averaged on a time scale driven by operational requirements. Because of the various time units used, care must be taken in dimensional balancing. Therefore, if customer throughput must match customer input on a daily basis, we can write

$$\frac{C \ \ comparisons / \sec * O \ \ operational \sec s / day}{P_{sys} \ * N \ comparisons / finger * m \ fingers / customer} = I \ customers / day \tag{10}$$

We note that the penetration rate, P_{sys}, is a percentage, and, therefore, non-dimensional.

9.7 The Philippine AFIS Benchmark Test

The Republic of the Philippines Social Security System (SSS) Identification Card Project AFIS benchmark test was conducted in May, 1997, with four international AFIS vendors, a fifth vendor withdrawing immediately prior to the test. The goals of the test were to measure penetration rate, bin error rate, and single comparison false match and false non-match rates for each vendor. We[36] did not attempt to measure hardware comparison rate, as the conditions of the contract required the guarantee of minimum throughput rate performance. The benchmark was undertaken in support of a national social security card project, with an anticipated eventual enrollment of 20,000,000 cardholders at an enrollment rate of 20,000 people per day when the full enrollment is reached. The system will use gender-based filtering and four fingers (left and right forefingers and thumbs) for enrollment.

9.7.1 Fingerprint Images

To facilitate the test, we collected three sets of images: "training," "practice" and "test." All images were taken from SSS adult employee volunteers, each giving eight prints at each session, thumb through ring finger of each hand. The volunteers were primarily managerial and clerical workers, although some volunteer laborers were solicited, as well. Each volunteer signed a consent form authorizing release of the collected data. The collection was supervised by three SSS employees. No personal data was collected with the prints other than gender; 55% of the volunteers were women.

[36] This author participated in the Philippine test as a paid consultant during the period of performance of the FHWA-sponsored study of this report. No FHWA–supported time or resources were used in the Philippine test. The Philippine government has given permission for the test results to be disseminated provided that the participating vendors are not named.

Database bookkeeping was accomplished by assigning each volunteer a collection number. Handwritten data sheets connecting volunteers with collection numbers was maintained by the supervising employees and have since been destroyed.

Prints were imaged with an Identicator DF-90 "flat" scanner, believed to be "Appendix G" compliant and an "MRT" frame grabber in a lap-top computer. Front-end quality control software from Identicator was employed. Database management software was supplied by Identicator for this project. The prints were stored, using loss-less compression, as "TIFF" images. Some image quality loss, attributable to frame-grabber noise during collection, was noticed in the upper right hand quadrant of most images.

The "training" data consisted of 4080 prints taken from 510 volunteer employees of the Social Security System over a three-week period. It was our original intent that the "training" data set be "clean," meaning free from duplicate images. Subsequent analysis by the vendors indicated that there were, in fact, 4 repeated prints in the set made by inadvertently inaccurate finger presentations by volunteers which were not corrected by the supervisors.

In collecting the 4080 "training" images, we were allowed to physically touch the volunteers, manipulating their fingers on the scanner and applying slight pressure with the intent of obtaining the highest print quality possible as judged by the quality control software. Moisturizing compound was applied as needed. In general, three or more prints were collected from each finger of each volunteer, although the training data set consisted of only one image from each collected finger.

A second, "test," data set of 4128 images was collected from 506 volunteers, 409 of whom were included in the training set. Although image quality was checked and moisturizing compound applied as needed, somewhat less care was generally taken to provide high quality images. Collection of the "test" set commenced one week after completion of the "training" set collection and was finished within three weeks. Consequently, individual volunteers were imaged at an interval of one to six weeks between the test and training sets. The test set contained 10 duplicate ensembles (80 prints) imaged from 10 volunteers in a separate session several weeks after the completion of the collection of the other images.

The order of the files and the file names were scrambled to prevent a determination of correlation between "test" prints and "training" prints or correlations within the "test" set, and a highly-secret key was created linking the "test" and "training" prints.

The third, "practice" set of 80 images was taken from 10 volunteers whose prints were in the "training" data set. The file names given these images were adjusted to identify them with their matching image files in the "training" set.

Both the "training" and "practice" data sets were mailed to the vendors several weeks prior to the tests. The "test" data set was hand delivered to the AFIS vendors on the day of the benchmark test. In all cases, testing was completed within the day.

9.7.2 Test Requirements

Prior to receipt of the "test" images, the vendors were required to supply the binning results for the "training" images. Vendors were allowed to report either "hard" or "soft" binning results, provided that enough information was supplied for analysis. By "hard," we mean the assignment of each print to one or more discrete bins. By "soft," we mean the assignment of numerical values to each print representing in some way a probabilistic binning assignment.

Vendors were required to report the binning assignments of each print of the "test" set using the same format as used in reporting bins of the "training" prints. Then vendors were required to match the "test" to the "training" prints, again reporting either "hard" or "soft" results. A "hard" result was a "match" determination between files. A "soft" result was a numerical similarity measure between files. Vendors choosing to return "soft" results were required to submit a 4080 by 4128 matrix of similarity measures.

9.7.3 AFIS Performance Results

Matching results were evaluated first. Only one of the four vendors (Vendor B) submitted the complete 4080 by 4128 similarity matrix in unedited form. The other vendors chose to replace low entries with zeros, possibly not computing similarity scores where bin assignments were incompatible. One vendor returned zeros for scores below an extremely high threshold, ultimately returning less than 4500 non-zero scores.[37] We computed single comparison false match and false non-match errors as a function of threshold for all vendors using the secret key.

There was significant correlation between all vendors regarding about eleven false matches. Consultation with our fingerprint expert confirmed that eight of these were in fact correct matches, indicating errors in our collection/record keeping procedure. The remaining three false matches were interestingly the false match of fingers from the correct individual, indicating the failure of our underlying assumption of independence between the fingerprints of a single individual. For this reason, we chose to disregard false matches when made from the correct individual. On this point, all vendors were affected about equally.

We have no assurance that the editing of results by vendors was done without reference to print binning. Consequently, we made the decision to divide the number of false match errors at each threshold by the number of non-zero cross-comparisons actually returned.

[37] Total number of returned non-zero scores: A=24,480; B=16,777,216;C=4445;D=111,181

Results, without error bounds[38], are shown as Figure 3. The results of Vendor A are interesting in that they were independent of chosen threshold over a large range of threshold values. Vendor A had no false matches at any reasonable threshold, so increasing threshold had no effect on the FMR. Genuine distributions are often bimodal, with the second mode coincident with the single mode of the impostor distribution. The distributions of Vendor A were disjoint, except for the overlap of the second mode of the genuine distribution with the mode of the impostor distribution. Therefore, decreasing the decision threshold had no impact on the false non-match rate until the threshold was well inside the impostor distribution, thus driving the false match rate sky high. So for all reasonable values of the threshold, the number of false matches remained at zero with about 2% false non-matches. It can be stated with 95% statistical confidence that the false match rate of vendor A was under 0.01%. It might be that the false match rate is even lower, but lack of returned match scores prevent us from making that determination. Vendor B returned 16,000,000 cross comparisons with only one false match, indicating a 95% statistical confidence of a false match rate of under 3 in 10 million ($3x10^{-7}$), but with a false non-match rate approaching 20%.

Binning results were also evaluated. All vendors submitted "hard" binning results, with one vendor submitting results of two "hard" binning procedures. Bins assigned to "training" prints were compared, using the secret key, to bins assigned the "test" prints and inconsistencies leading to binning errors were noted. Binning error rate as a percentage of the 3267 matching pairs was calculated. The two "hard" approaches for the single vendor were evaluated as though they were independent.

One vendor submitted "soft" results from a second binning approach, in addition to "hard" results from the first. These results were evaluated using a variety of thresholds.

Penetration rate was calculated empirically from the equation

$$P = \frac{\sum^{N_2} test\ prnts \sum^{N_1} training\ prnts\ with\ common\ bin}{N_1 * N_2} \tag{11}$$

where N_1 is the number of training prints and N_2 is the number of test prints.

The results of the binning test are given as Figure 4. Bin error rates vary from about three per thousand to about 50 per thousand. Penetration rates vary from about 46% to 60% based on method employed. The single soft binning method was not considered independently, but rather appended to the hard results from the same vendor.

[38] Error bounds were not included because of significant bias in the presented results. The bias is a result of the truncated result reporting by the vendors. Consequently, the "false match" rates must be interpreted cautiously. They are correct, however, well within an order of magnitude, which is acceptable for performance prediction in our application. The single point result in the bottom left-hand corner of Figure 2 was moved from the axis (there were no false-match errors in results received from this vendor) to indicate the uncertainty caused by the small number of returned comparisons.

Placement closer to the lower left hand corner of the graph indicates generally better performance.

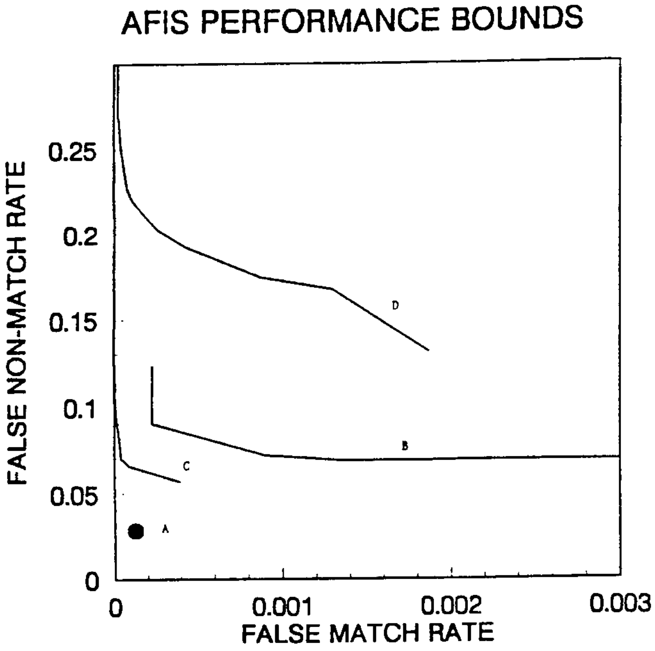

FIGURE 3

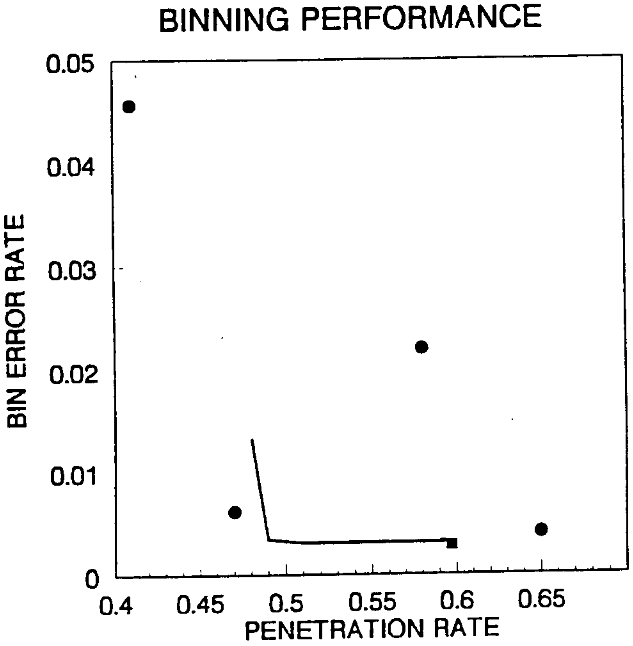

FIGURE 4

9.8 Performance Prediction in the CDL Environment

With this data, we can predict throughput and error rates for a centralized fingerprint system used in conjunction with CDLIS. Based on the Philippine test, we'll assume that a vendor can maintain a single finger false match rate of under one in one million while keeping the single finger false non-match rate below 10%. Further, let's assume a single finger penetration rate of 50% with an associated bin error rate of 1% and that, owing to a predominance of male commercial drivers, gender-based filtering is not helpful. The ultimate enrollment size of the centralized database will be 8.5 million drivers, with 2.5 million renewals and new issuances annually.

We will first show that a single finger system cannot meet the revised functional requirements. A searched print can be falsely not matched because of a binning error or because of a single comparison false non-match. The probability that a single searched print has neither can be expressed as

$$1 - FNM_{sf} = (1 - \varepsilon_{bin\ ensemble})(1 - FNMR) \tag{12}$$

where FNM_{sf} is the probability that the system falsely does not match a single searched finger, $\varepsilon_{bin\ ensemble}$ is the probability of a binning error over the ensemble, and FNMR is the single comparison false non-match rate. The explicit dependency of FNMR and FNM_{sf} on threshold, τ, has been dropped for notational simplicity. Providing that both FNMR and $\varepsilon_{bin\ ensemble}$ are small, equation (12) can be rewritten as

$$FNM_{sf} = \varepsilon_{bin\ ensemble} + FNMR \tag{13}$$

In a single print system, the ensemble bin error is by equation (6), just the single finger bin error rate. Therefore, in our hypothetical single finger system, the system false non-match rate is 1% + 10% = 11%. This is only slightly higher than functional requirement 4 mandating no more than a 10% false non-match rate in the recognition mode. In the verification mode, however, the probability of a false match is simply the false match rate, which in this case is 10%, significantly higher than the goal of 1%.

The probability that a single searched print is not matched against any print in the searched database is

$$1 - FM_{sf} = (1 - FMR)^{P_{sys} * N} \tag{14}$$

where FM_{sf} is the system single comparison false match rate, FMR is the single comparison false match rate, P_{sys} is the penetration rate, and N is the size of the database. Again, explicit dependency of FM_{sf} and FMR on threshold, τ, has been dropped for notational simplicity.

Equation (14) can be rewritten as

$$FM_{sf} = 1-(1-FMR)^{P_{sys}*N} \tag{15}$$

In a single print system without gender-based binning, the system penetration rate is simply the single finger penetration rate, in this case assumed to be 50%. With a false match rate assumed to be 10^{-6} and N at 8.5 million, the system false match rate becomes, by (15) above, almost 99%. Even worse, the expected number of false matches per search can be given by

$$E[FM] = P_{SYS} * N * FMR \tag{16}$$

which computes to about 4 in this example. Clearly, a single finger system cannot meet the functional requirements.

Now we will show that a two-finger system can approximately meet the functional requirements. With two fingers, we can use ensemble binning, which by equation (6), will give us a penetration rate of 0.25. If we use a two-finger search, then a system false non-match requires two single finger false non-matches. Under the assumption of error independence, the probability of that happening can be given by

$$FNM_{system} = (\varepsilon_{bin\ ensemble} + FNMR)^2 \tag{17}$$

which in our case yields a system false non-match rate of less than 2% in the recognition mode, meeting the functional requirement. For verification, the availability of two fingers implies a false non-match rate of $FNMR^2$, computing to 1%, also meeting the functional requirement. It is noted that the false non-match rate is independent of database size, N. Consequently, this result will hold for decentralized, state-based systems.

If the bounding system match policy requires a match on both fingers for a system match to be declared, the probability of a system false match, FM_{system} ,occurring is

$$FM_{sytem} \approx P_{sys} * N * FMR^2 \tag{18}$$

In our case, the recognition false match rate computes to $0.25*8.5*10^6 *10^{-6} *10^{-6} = 2*10^{-6}$, which does not meet the functional requirement by a factor of 2, yielding 2 false matches per one million applicants. On the other hand, if the single finger false match rate is taken as $0.7*10^{-6}$, only 30% lower than the estimate used here (and well within our estimation uncertainty), the functional requirement is met. As the false match rate is linear in N, performance for decentralized, state-based systems will be better than that computed here for a centralized system.

Some have criticized this approach by saying that (17) and (18) cannot be met simultaneously, because equation (17) does not account for a correct match followed by a single false non-match. There is no requirement that (17) and (18) be implemented with a single, fixed threshold value, τ. Appropriate choice of system decision policy, particularly given the liberal false non-match rate allowed by the functional requirements, will allow both false match and false non-match requirements to be simultaneously met. The verification false match rate is, depending upon system policy, no worse than the single finger false match rate of 10^{-6}, more than meeting this functional requirement.

The hardware comparison rate required to support the projected throughput rate of 2.5 million per year can be projected using equation (10). Assuming 80,000 operational seconds per (22 hour) day and 250 operational days per year, the required comparison rate is

$C = 2.5*10^6/250/80{,}000*0.25*2.5*10^6 *2= 150{,}000$ comparisons per second

This is a lower bound on the true requirement, which will be greater owing to higher than calculated penetration rate caused by bin correlations and the additional computations required by matches. Nonetheless, this value is well within the capabilities of current hardware systems. This implies that overnight operation will be possible, meeting the 72 hour turn-around time specified in functional requirement 5. Using a current "rule of thumb" of many dollars per match per second, central processing hardware costs would approximate a million dollars for a national system. Of course, for decentralized systems, the hardware requirements will be even more relaxed. Total system costs, however, depend upon far more than the centralized processing hardware.

Transmission of approximately 10,000 two-print records would be required on an average day. Assuming uniform distribution of this transmission over an 11 hour day and about 30kbytes for each record in the NIST/ANSI data format, approximately 30kbytes of data would require transmission each second. Even multiplying by a safety factor of 10, this is a trivial data rate for AAMVANet, NLETS, or the internet communications networks.

We need not make any additional computations to determine the maximum "start-up" speed of the system. The throughput rate of 2.5 million applicants per year was based on a presumed 4-year renewal cycle. A start-up policy of simply enrolling drivers in the system at the time of renewal would lead to complete enrollment in 4 years with no additional computational burden on the system. In fact, during the early years of such a 4-year start-up period, the computational burden would be considerably reduced owing to the small number of prints in the database.

Although there is no AAMVA functional requirement for "over-the-counter" issuance, it is interesting to inquire as to the hardware requirements of such a system at the Federal level. Replacing the 22 hour day with an 11 hour day (allowing for 3 time-zones in 8 hour-per-day operation), the above equation shows that a machine match speed of at least 300,000 comparisons per second would be required. Most likely, this underestimates the true requirement by at least a factor of 2, owing to uneven temporal distribution of the licensing demand and under-computation of the penetration rate. A system designed to make 600,000 comparisons per second would be bigger than any AFIS now in existence, but is probably technically feasible

We can conclude that, regardless of the choice of a centralized (Federal) or decentralized (state) system, a two-finger fingerprinting system can meet the target false match and false non-match rates of the functional requirements in both recognition and verification modes, and that hardware requirements are well within the current state of AFIS technology.

10.0 A SURVEY ON THE USE OF FINGERPRINTING FOR DRIVER'S LICENSE APPLICATIONS

In the Spring of 1997, we conducted a telephone survey of all AAMVA U.S. jurisdictions. All U.S. departments of motor vehicles were contacted and information was collected as to whether or not these departments are implementing a fingerprint collection program in their driver's license issuance practices. The following questions were asked and the answers of the cognizant drivers licensing official were recorded:

1. Are you currently fingerprinting?
2. Is it voluntary or mandatory?
3. Which finger(s) are you using?
4. Which technology (hardware) are you using?
5. What is the process and environment used to acquire templates/samples (looking for unhabituated/attended/cooperative, etc.... information)?
6. Is the data stored on cards and/or in a central database?
7. Are you using the data/records? If so, what is the system and process used to access?

As of the Spring of 1997, seven states were collecting fingerprint information. Of the seven, five were using the fingerprints in their drivers licensing programs. Alabama, California, Hawaii reported collecting right thumbprints. Florida collected left thumb information and Texas uses both thumbs. Colorado used the right index finger and Georgia collected images from both index fingers. Complete results are tabulated in Appendix K. Between the completion of the survey and the date of this report, both Florida and Alabama have announced the suspension of the fingerprinting programs.

We also learned in the course of this survey that West Virginia and Polaroid have entered into a contract that will create a driver's license using facial recognition in combination with digitized finger images. A pilot program is expected to be running in the summer of 1997 with full operation planned for the fall. West Virginia issues about 500,000 licenses each year. For this system, we have not attempted an error rate analysis similar to that of Section 9.8 above as basic single image false match and false non-match rate estimations are not available from any independent source for any facial recognition system. However, based on the analysis of Section 9.8, we question whether a single image system is reasonable for any biometric approach at this scale.

11.0 SYSTEMS ISSUES AND COMPETING ARCHITECTURES

We have not yet discussed architecture issues. There are two fundamental ways in which the system could be constructed: on the federal level and on the state level. A state-level system could have two forms: one with centralized communication and one with distributed communication. We will briefly discuss each.

11.1 A Federal-Level System

The most straightforward and cheapest approach to the identification of commercial drivers would be a national system, much like CDLIS, which electronically holds the feature vectors (most likely, minutiae) of all licensed commercial drivers. The feature vectors would be "pointers" by which the database could be accessed. For searching, it is not possible to have any other point record pointing to this template, so centralized submission and storage of at least this fingerprint-related data is required. Recalling that fingerprint images cannot be reconstructed from the feature vectors, the original images would remain stored in the states which collected them and accessed only if a prosecution for driver's licensing fraud was indicated. However, because each state might be using different fingerprinting contractors with incompatible feature vector formats, the fingerprint images, collected during the licensing procedure using scanners of standardized image quality, would need to be transmitted in compressed form to the central site for feature extraction. The states would archive the images, while the central site would extract the features, then discard its copy of the original images. States objecting to the transmission of compressed images could send the features only, but would be required to use the contractor-specific feature extraction software mandated by the national system manager.

A commercial driver applying for a new license or a renewal would have copies of his/her images sent to the central site, converted to features and scanned against the existing database. The transmitted copies of the images would then be destroyed. In the case of a new license, if no match was found, the license could be issued and the features stored in the database. In the case of the issuance of a duplicate or a renewal, a match should only be found against the registered license holder. Any other matches would indicate multiple license fraud. This approach to scanning the entire database for both new licenses and renewals provides a "double check" against multiple issuances. To be effective, all states would be required to participate. A non-match during the renewal or duplicate issuance process might indicate single license/multiple driver fraud.

Could such a large centralized system be built and would it work? Section 9.8 of this report considered the error and throughput rates of such a centralized system and showed that the AAMVA functional requirements could be approximately met with current technology.

An advantage of a federal system would be that the federal feature extraction method would become a *de facto* standard, allowing for the feature record to be encoded on the license for roadside matching. Thus roadside biometric verification, linking the driver to the license, could be accomplished nationally.

As to be discussed in Section 12.3 of this report, several AAMVA states have indicated an unwillingness to release a driver's fingerprints to a central system. It is not necessary that the fingerprint image itself be sent to the central system, but the extracted features must be. States would have the option of submitting, in place of the fingerprint image, only the feature template extracted using the algorithm of the vendor of the centralized system. The fingerprint cannot be reconstructed from this template.

What would be the marginal cost of such an identification system (excluding roadside verification function) if created as an adjunct to the CDLIS system? Informal industry estimates indicate that initial expenditures of $10M to $20M would be required for hardware, software, system integration and training.

We conclude that there are no technical barriers to the implementation of such a system, but the political barriers may be formidable, requiring additional enabling federal legislation.

11.2 A State-Level System

A state-level system would consist of 51 jurisdictional, "stand-alone" AFIS administered and funded by the various states for the collection and processing of fingerprints for commercial driver's licenses. These systems could be linked together in either of two differing ways: through centralized or distributed communication.

11.2.1 The Distributed System with Centralized Communication

A state-level system with centralized communication would have each state maintain and control its own commercial driver AFIS system. Each state could have a different contractor and different feature extraction protocols, but each would collect data at the nationally-mandated image quality standard. The fingers to be used will be standardized across all states, although these will be "minimum standards," allowing each state to collect additional prints, if desired. All states must have the capability of both sending and receiving WSQ-compressed, ANSI/NIST format images to and from other states. Duplicate or replacement licenses would be issued only upon the verification against the state's own database of the applicants fingerprint. Single license/multiple driver or driver substitution fraud could be detected with no interstate transfer of data.

When a driver applied for a new license, the fingerprint image, compressed using the standardized WSQ method, would be sent by AAMVANet , NLETS or internet to a centralized communication site for distribution to the independent systems in all the other jurisdictions. Any jurisdiction finding a match would report the find directly to the originating state.

The centralized communication site would have to transmit each image 50 times, leading to a centralized output of several hundred kbytes per second, a trivial load for a large server. Input data rate at the state and central sites would be at the average rate of one image every 3 seconds. California, the largest state with about 600,000 commercial driver's licenses (CDLs), would be conducting about 50,000 comparisons per second (considering a 25% penetration rate), requiring a mid-sized system.

The capability for roadside verification of the driver's license could be at the discretion of the states. Whether verification capability is federally mandated or not, because of the state-by-state variability of systems and protocols, verification could only be done within the state of issuance.

The political advantage of this system is that states would only release images for immediate search, not for storage in any form outside the state. Each state would maintain complete control of all its images and derived features. The disadvantage would be the total cost of the system, with loss of the economies of scale of the centralized system. The effectiveness of this system would be identical to the centralized system, provided that all states participated.

There are no unresolved technical issues affecting the feasibility of such an architecture. AAMVA functional requirements could be met by such a system. The total cost of all the systems would exceed that of a single federal system, however.

11.2.2 The Distributed System with Direct Communication

The second approach to a state-level system identical to the first, except that compressed fingerprint images would be sent directly by the collecting state only to selected, participating states for search. Transmission of the compressed images could be by AAMVANet, NLETS or internet. Receiving states could charge originating states a fee for searching of an image against their database. This system would require no generalized transmission of fingerprint images, giving each state tight control over which images would be sent to which states for search. Further, states could participate or not as local politics required. This system would be effective against renewal and single-license/multiple-driver fraud. Effectiveness against multiple license fraud would be limited, however, if not all states participated.

Because the search will be over fewer records, image quality standards will not be as important. It may be possible to operate such a system with lower image quality standards. "Minimum standards" for the fingers to be used must be established, however. States wishing to participate in the system must have the capability of both sending and receiving WSQ-compressed, ANSI/NIST format images to and from other states. Because such out-of-state searches would be relatively infrequent, transmission bandwidth would not be an issue. AFIS size would be limited to just the number of commercial drivers in the state, the largest being about 600,000, which is now considered reasonably small by vendor standards. There are no substantial technical challenges to any aspect of start-up or operations.

The advantage of this approach would be to allow each state now collecting prints and/or encoding them on driver's license documents to upgrade their current system only where necessary. States could expand current non-CDL fingerprinting systems to meet this requirement, or procure new systems for both CDL and non-commercial driver licensing. States would maintain complete control of their systems, data and most standards and could raise funds by performing searches for other states. The capability for roadside verification within the state of issuance could be at the discretion of each state.

There are no unresolved technical issues affecting the feasibility of such an architecture. AAMVA functional requirements could be met by such a system.

12.0 LEGAL CONSIDERATIONS

The legal and political considerations of this project are far more difficult than the technical ones. As stated multiple times in this report, there appear to be no major technical problems preventing implementation of either a centralized or a state-based system for the biometric identification of commercial drivers. The major problems appear to be entirely legal and political. Political questions, relating to assessment of the public and governmental willingness to pay for and implement this system, establishing the need for the system as a tool of policy enforcement, and determining the willingness of commercial drivers to accept it, are beyond the scope of this study. Yet, the ultimate fate of the proposed commercial driver biometric identification system rests entirely on the answers to these non-engineering questions.

It is within the scope of this study, however, to look at current laws and legal precedence and ask if such a system would conflict with any Federal or state statutes or court findings. We have done this in Appendix L, a paper titled "Reconciling Government Use of Biometric Technologies with Due Process and Individual Privacy." In this section, we will examine several legal issues with potential impact on this project, starting with the Constitutional proscriptions against self-incrimination, illegal search and seizure, and denial of due process.

12.1 Search, Seizure and Self-Incrimination Considerations

We have discovered several U.S. Supreme Court rulings upholding the right of the government to require the submission of a biometric measure or biological sample as a prerequisite for the granting of a privilege or for the enforcement of public safety. The Supreme Court has ruled that such required submission does not violate Bill of Rights' proscriptions against self incrimination (fifth amendment) or illegal search and seizure (fourth amendment).

For example, in the case, *Breithraupt v. Abram,*[39] decided in 1957, police had taken a small blood sample from an unconscious person involved in a fatal car accident. The Supreme Court ruled this extraction was constitutionally permissible, stressing that clinical blood extraction was not significantly intrusive and had become both commonplace and accepted by society. Nine years later, the Court reiterated this point in *Schmerber v. California,*[40] by recognizing that both federal and state courts have held that the right against forced self incrimination does not extend to forced subjection to fingerprinting,[41] photographing, or physical measurements, nor to forced writing,[42] speaking, standing, walking or gesturing for identification purposes.[43, 44]

The Supreme Court's positions on fourth and fifth amendment issues have generally followed the path of *Breithraupt* and *Schmerber* in allowing non-intrusive, non-verbal data collection in criminal settings. It is, therefore, likely that courts will rule that biometric data taken in the non-criminal context of commercial driver's licensing, even when the data may later be used in a criminal proceeding, is not so obtrusive that it violates elements of privacy inferred within the fifth amendment's self incrimination clause or constitutes an illegal search or seizure.

The most direct legal ruling on the appropriateness of fingerprinting as a requirement for obtaining a driver's license comes from the 1986 California Supreme Court case of *Perkey v. Department of Motor Vehicles.* As a case from a state Supreme Court, the decision, of course, is not binding on the rest of the country, but it does indicate how one court considered a challenge of the procedure. Perkey contended that the California Department of Motor Vehicle's mandatory fingerprint requirement violated her fourth amendment guarantee against unreasonable search and seizure. In disposing of this argument, the California Supreme Court examined the existing case law and concluded the fingerprint requirement did not exceed fourth amendment thresholds for obtrusiveness. Its inquiry first examined whether fingerprinting involved the type of intrusive invasion of bodily integrity that has, in the past, been found to violate either the due process clauses of the fifth and fourteenth amendments or the implicit privacy guarantees of the fourth amendment. The court concluded that fingerprinting alone does not infringe upon an individual's right to privacy, holding that fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search.[45] Unlike forcible stomach pumping[46] or the forced taking of a

[39] 352 U.S. 432 (1957).

[40] 384 U.S. 757 (1966).

[41] See *New rk v.Quarles*, 467 U.S. 649, at 671 (1984), Justice O'Connor concurring, noting how an interrogation does not offend the values underlying the fifth amendment any more than compulsory taking of blood samples, fingerprints or voice exemplars.

[42] Gilbert v. California, 388 U.S. 263 (1967).

[43] See also *U.S. v Chibbaro*, 361 Fed. 2d 365 (Cal. 3d Cir.) (1966) and *People v Graves* 64 C.A. 2d. 208 (1966).

[44] See Weintraub, "Voice Identification, Writing Exemplars and the Privilege Against Self Incrimination," 10 Vanderbilt Law Review (1957).

[45] *Perkey*, at 191.

semen sample[47], both previously disallowed by the courts as unreasonable, the physical process of taking a fingerprint does not require penetration beyond the body's surface.[48] Therefore, the court ruled that fingerprinting does not readily offend the principles of reasonableness under the fourth amendment.[49]

Consequently, it is our opinion that any challenge to a fingerprinting requirement for commercial drivers, based on a claim that self-incrimination or illegal search and seizure was inherent to the collection process, would not be accepted by the courts.

12.2 Due Process Considerations

The fifth amendment prohibits the denial, by the Federal government, of life, liberty or property to any person without the "due process of law." The fourteenth amendment extends this protection against actions by states, as well. Because a biometric identification system applied to commercial drivers for the enforcement of driver's licensing laws could result in the denial of a license application or renewal, we investigated the legal requirements for due process engendered by such a denial.

Philosophically, two rationales have been used to justify the importance of due process in a democratic society:[50] the intrinsic and the instrumental approaches. The intrinsic approach suggests that society gains an important moral benefit by allowing individuals to participate in the governmental processes affecting them. As Justice Frankfurter opined in *Marshall v. Jerrico*,[51]

> "no better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it. Nor has a better way been found for generating the feeling, so important to a popular government, that justice has been done."

The second approach to due process, the instrumental, focuses less on the right of people to be part of a decision making process affecting them and more on the need to assure that rules for distributing government services are accurately and consistently followed. The instrumental approach creates due process requirements to minimize substantially unfair or mistaken decisions that lead to deprivations of entitlements conferred to people by law. Under the instrumental approach, the purpose of due process

[46] In *Rochin v. California*, 342 U.S. 165 (1957), the Supreme Court declared that forcing a drug suspect to have his stomach pumped was police behavior that shocked the conscious of a civilized society and, therefore, violated the fourth amendment ban against unreasonable searches and seizures.

[47] *People v. Scott*, 21 Cal. 3d. 284 (1978).

[48] *Perkey*, at 191.

[49] *Id.*

[50] In *Carey v. Piphus,* 435 U.S. 247 (1978), Justice Marshall wrote that the two concerns of procedural due process are the prevention of unjustified or mistaken deprivations and the promotion of participation and dialogue by affected individuals in the decision-making process, at 259-262 and 266-267.

[51] 446 U.S. 238 (1980).

is not primarily to assure participation by affected parties, but rather, to assure that government makes an accurate decision.[52]

In both intrinsic and instrumental approaches, due process protections increase as the individual identities of the affected parties becomes clearer[53] and as the effect of the government decision becomes increasingly under the control of an identifiable decision-maker. Therefore, under both approaches, an individual has a right to greater due process of law in challenging an adverse government decision than would a group.[54] Similarly, an individual has a right to greater due process of law as the severity and harm of the adverse decision increases.[55]

In the 1970 case of *Goldberg v. Kelly,*[56] the State of New York had terminated welfare benefits without first allowing the individual an evidentiary hearing. The U.S. Supreme Court ruled against New York, arguing that because both the federal Aid to Families With Dependent Children and New York's Home Relief programs were statutorily created entitlement programs, these forms of assistance should be considered more a form of property than a gratuity.[57] Because welfare benefits give a recipient the means to survive, the Court ruled that benefit denial without a pre-deprivation evidentiary hearing would violate due process. The Court reasoned that the nature of the entitlement was so fundamentally linked to the basic survival of the individual, termination without a prior hearing would gravely impair a basic right to life and liberty.[58]

During the early 1970's, the Court expanded the concept of a pre-termination hearing in several areas: revocation of parole,[59] probation,[60] early release for good behavior by inmates,[61] suspension of a driver's license,[62] high school suspension,[63] public

[52] Tribe, *Supra* note 6, at 667.

[53] In *O'bannon v. Town Court Nursing Center,* 447 U.S. 773 (1980*),* which dealt with the unwilling transfer of elderly patients form a decertified nursing center, Justice Blackmun, in his concurrence, noted that as individuals are more specifically singled out from a larger group, their due process rights grow stronger, at pp. 800-801.

[54] *Id.*, at pp, 799-800. Justice Blackmun noted that as "governmental action affects more than a few individuals, concerns beyond economy, efficiency, and expedition tip the balance against finding that due process attaches. We may expect that as the sweep of governmental action broadens, so to does the power of the affected group to protect its interests outside rigid constitutionally imposed procedures."

[55] *Id.*, at 803. When a government action entails a serious likelihood of added stigma or of harmful treatment that increasingly puts an individual at risk of death or grave illness, government action must include input by those affected by the decision.

[56] 397 U.S. 254 (1970).

[57] *Id.*, at 262, n. 8.

[58] The Court noted that welfare provides the means to obtain essential food, clothing, housing and medical care and that terminating the welfare benefits, rightly or wrongly, will have the inevitable effect of depriving an individual of the very means by which to live. Therefore, considering the grave consequences, terminating welfare benefits for which an individual had statutorily qualified, without first allowing the individual to demonstrate the decision to be erroneous, violated constitutional due process.

[59] *Morrissey v. Brewer*, 408 U.S. 471 (1972).

[60] *Gagnon v. Scarpelli*, 411 U.S. 778 (1973).

[61] *Wolff v. McDonnell*, 418 U.S. 539 (1974).

posting of people unfit to consume alcohol,[64] housing evictions from public projects,[65] repossession of property,[66] garnishment of wages[67] and denial to students of state residency eligibility while attending college.[68]

Because denial of a commercial driver's license on the basis of a biometric measurement, perhaps in error, could cause the loss of a means of livelihood, we believe that the courts would require a pre-termination hearing for the aggrieved individual.

12.3 State Laws Regarding Inter-State Exchange of Biometric Information

In the current absence of any federal legislation impacting the collection and dissemination of fingerprints for driver's licensing purposes, state laws rule supreme. Some states currently collecting fingerprints are legally unable and/or unwilling to release those prints to other states or federal agencies. We will mention here both California and Georgia. It is the opinion[69] of the General Counsel's Office of the California Department of Motor Vehicles that the federal government does not have the legal mandate to require the submission of fingerprints on commercial drivers to a centralized system. Without mandating federal legislation, California would be unwilling to release those prints.

The Georgia Department of Public Safety is prohibited by from releasing fingerprints to driver's licensing agencies of other states. According to Section 40-5-2 (c)(1.)(D) of the Official Code of Georgia (Annotated) "...personal information furnished to the driver's licensing agency of another state shall be limited to name, address, driver identification number, and medical or disability information." It is the opinion of the Director of the Legal Section that this section forbids the release of fingerprints on commercial drivers to other states even for the purpose of enforcing the "one-driver, one-license, one-record" provisions of the Commercial Motor Vehicle Safety Act. The Director has no current opinion on the release of fingerprints to the federal government for this purpose, however.

Texas reports[70] no legal restrictions on the dissemination of collected fingerprints. Colorado reports[71] "no specific statutory prohibition" against the dissemination of prints

[62] *Bell v. Burson*, 402 U.S. 535 (1971).

[63] *Goss v. Lopez*, 419 U.S. 565 (1975).

[64] *Wisconsin v. Constantineau*, 400 U.S. 208 (1971).

[65] *Caulker v. Durham*, 433 F.2d. 998 (4th Cir., 1970) cert. denied 401 U.S. 1003 (1971).

[66] *Fuentes v. Shevin*, 407 U.S. 67 (1972).

[67] *Sniadach v. Family Finance Corporation*, 395 U.S. 337 (1969).

[68] *Vlandis. v. Kline*, 412 U.S. 441 (1973).

[69] According to AAMVA Biometrics Working Group member Marilyn Schaff, General Counsel, California Department of Motor Vehicles.

[70] Mr. John Hall, member of the AAMVA Biometrics Working Group and Inspector, Texas Department of Public Safety.

[71] Mr. John Duncan, Assistant Director, Colorado Motor Vehicle Division.

for the purpose of non-criminal searches, but would require the opinion of the state Attorney General before prints could be shared with other AAMVA jurisdictions.

It is clear that voluntary participation in a multi-state CDL fingerprinting system, even by states currently collecting them, will require a change in at least some state laws. Mandatory participation will require enabling federal legislation.

13.0 OUR RESPONSE TO THE 24 QUESTIONS OF THE ANPRM

1) How many drivers currently operate in defiance of the law?

The 1997 New York CDLIS Effectiveness Study was unable to document any commercial drivers operating with multiple licenses. Part of the difficulty in documenting the problem is the lack of an effective methodology for discovering multiple issuances. We have no suggestions in this regard. The New York study did not address the problem of a single license operating with multiple drivers. Such a case leading to a traffic fatality has been documented by the Alabama Department of Motor Vehicles, but there has been no national study aimed at quantifying this problem.

2) How extensive will this problem be when the program is fully implemented and all CDL holders are entered into the CDLIS?

CDLIS is now fully implemented. There are currently approximately 8.5 million driver records in CDLIS. Some of these may represent now inactive drivers. The CDLIS Effectiveness Study showed no drivers operating with multiple licenses, but did not study the problem of multiple drivers with a single license. We can conclude that the CDLIS has been effective in limiting multiple licenses. The Alabama case illustrates, however, that there is still a problem with single licenses with multiple drivers.

3) On what basis are the above estimates of the size of the problem made?

We have no basis upon which to estimate the size of the total problem.

4) What alternatives besides the biometric identifier can be used to reduce or eliminate the problem?

It may be that the current CDLIS system and the penalties for holding multiple licenses have decreased the size of this problem. But again, given any baseline (pre-CDLIS) studies and a lack of effective methodology for discovering multiple issuances, we cannot give a conclusive answer to this question.

5) Since the CDLIS supports a broad comparison of identifying information, does internal comparison of individual identification records, in conjunction with severe penalties, provide ample reason for drivers not to seek multiple licenses?

According to the New York CDLIS Effectiveness Study, it does.

6) How much will such a system cost in terms of hardware, software, personnel, training, and impacts on existing state licensing procedures?

If "over-the-counter licensing" is not required, up-front capital and implementation costs for a national system would be on the order of $10M, based on informal estimates from the AFIS vendor community and the recent experience of the Philippine Social Security System. Cost of state systems could run between $100,000 and $2M, depending upon the number of commercial drivers within the state. The addition of "roadside" detection capability would increase the price of the system.

7) What factors are most likely to increase costs of the system?

The primary cost factors are the number of commercial drivers, the enrollment rate, the number of collection stations and the addition of any "roadside" collection and processing hardware.

8) What are the costs likely to be for making the system mandatory for all states as opposed to making it optional?

There is no support within the AAMVA Biometrics Working Group for a FHWA mandate for the biometric identification of commercial drivers. An administrative mandate without Congressional legislation would be challenged in court.

9) What are the benefits likely to be? a) In terms of money? b) In terms of "non-monetary" or social benefits?

We have been unable to quantify benefits of the system.

10) How much would each state be willing to pay each year for such a system? a) In terms of additional AAMVANet costs? b) In terms of within state costs? c) Both of these?

The AAMVA Biometrics Working Groups believes that the states are unwilling to shoulder any additional financial burden resulting from a biometric system aimed only at CDL holders.

11) How much would each licensee be assessed for such a system and how would this relate to total costs?

Assuming license renewal every 4 years and an 8 year life to the system, the assessment on the order of $1 per license could approximately pay for the system, whether state or Federal.

12) What is a tolerable error rate for both erroneously identifying a match when there is not one and not identifying a match that should actually be one?

A reasonable false non-match rate for a two-finger system is 1%. The false match rate is a function of the system size (see Appendix E), and consequently depends upon whether a federal or state system is contemplated. For a federal system with 8.5 million enrollees, a false match rate of 1 in one million applicants is a reasonable goal for a two-finger system.

13) How much additional time for conducting the match search is considered acceptable?

System cost is driven by search speed requirement. Consequently, this question can only be answered as a design trade-off with system cost (See Appendix F).

14) Under what conditions would it be acceptable to issue temporary licenses?

This question can only be answered by AAMVA.

15) What are the acceptable added costs per license, assuming limited and widespread use?

This question can only be answered by AAMVA.

16) What benefits would be achieved in having the biometric information available on the CDL in a form that could be read electronically?

If the information could be read electronically, the biometric could be used to verify the holder of the license at roadside stops within the state of issuance. Owing to the absence of standards for feature extraction, any biometric information on the CDL would be unreadable outside the state of issuance. Centralized encryption of the information on the license would give some protection against the problem of counterfeit licenses within the state of issuance. Eliminating counterfeit licenses and licenses with multiple drivers would require access at roadside to biometric information stored at a centralized site.

17) Should the establishment of such a system be made mandatory for all states?

The AAMVA Biometrics Working Group would be strongly opposed to a Federal mandate, particularly if unfunded.

18) If so, when should such a system be mandated?

There is no AAMVA support for mandating this system.

19) Are there privacy issues involved?

Privacy issues involving biometrics are covered in Appendix L.

20) Would there be any privacy distinctions between an AFIS and the retinal scan?

Retinal scanning may reveal peripheral health information on applicants, such as diabetes, macular degeneration, and possibly retinal changes associated with AIDS. No documentable health information is associated with fingerprints. Therefore, there is a privacy distinction between AFIS and retinal scan systems.

21) If problems are noted, what modifications would alleviate these?

We suggest that fingerprinting be adopted as the biometric measure for the identification of commercial drivers.

22) Who should have access to this data and for what purpose?

Access to this information beyond the driver's licensing and traffic enforcement community must be strictly limited. We strongly suggest that written policies be established permitting use of the biometric information only for the purpose of enforcement of the commercial licensing provisions of Federal and state law.

23) Is there vendor support to accommodate nationwide implementation and projected growth?

We believe there to be widespread vendor support for nationwide implementation of this system.

24) Should the FHWA merely specify performance parameters and leave vendors to develop requisite systems, or should the selection be restricted to existing system designs?

System functional requirements, throughput rates, and error rate goals should be specified, including interface requirements with existing systems. Further, the political choice of federal or state system cannot be made by vendors. Exact system design should be left to the vendors.

14.0 FINGERPRINTING AND THE REVISED FUNCTIONAL REQUIREMENTS

In this section, we will look at the possibility of meeting the revised functional requirements using a biometric identification system based upon fingerprinting.

Requirement 1: "... without increasing the net transaction processing time...by more than 30 seconds."

Working to our advantage, the system will be integrated into the licensing process, so additional data entry will not be required. The transaction time directly attributable to the fingerprinting will be limited to the collection of the two prints. Nonetheless, collecting two fingerprints of good quality from non-habituated users in 30 seconds will certainly be a challenge. In fact, some percentage of the population will undoubtedly not be able to supply two prints of satisfactory quality within this, or any, time interval. Consequently, if Requirement 1 is meant to apply to every transaction, it cannot be met. On the other hand, if it applies to the average transaction time for all users, there is hope. The 1990 Orkand study revealed that about one minute was required to collect each print[72]. Key to improvement will be the "human factors" element of the man-machine interface; that is, how self-explanatory and "user friendly" the hardware and software of the system is. This can only be worked out during the implementation process.

Requirement 2. "accurate, relatively unalterable, unique, physical characteristic...over an indefinite period of time."

The Philippine results cited in Section 9.7.3 of this report indicate that two finger systems are highly accurate with respect to both false match and false non-match error rates. The low false match rate also indicates compliance with the "unique" requirement. Popular knowledge indicates that fingerprints are stable over an indefinite period of time. Although the issue of automatic identification in adulthood of fingerprints taken in childhood remains open, it would not apply to the current question of identifying commercial drivers. Consequently, we can conclude that fingerprinting meets Requirement 2.

Requirement 3. "...unobtrusive to the applicant, socially acceptable... not endanger the health, safety, or welfare of any applicant."

The 1990 Orkand report included a survey of 9,709 participants in a fingerprinting and retinal scanning demonstration project. With regard to each technology, participants were asked their agreement, on a scale of one (very) to five (not at all), with several statements:

[72] Orkand (1990), op. cited, page IV-B-7

It is comfortable:	88%
It is safe:	92%
It is scary.	5%
It is threatening.	5%

The numbers next to the statements above indicate the percentage of respondents answering 1 or 2 with regard to electronic fingerprinting.[73]

In response to the question "Now that you have done this, do you feel that it is an okay procedure?" 98% answered "Yes" with regard to electronic and inked fingerprinting. In response to the question, "Do you feel that it is acceptable to use personnel identifying technologies to make sure that each driver can be issued only one license?" 95% answered "Yes."[74]

With regard to health and safety, we cannot postulate any mechanism whereby any of the finger scanning technologies would present any health or safety risk. Consequently, we can conclude that fingerprinting meets Requirement 3.

Requirement 4. "... previously tested for accuracy in an environment that proximates that of the CDLIS and with a less than 10% false non-match error rate in the recognition mode... (false match of) not more than one applicant in one million when the system is at the target enrollment level of 8.5 million. In the verification mode, the false non-match rate should be less than 1% with a false match rate of also less than 1%.

The Philippine benchmark test documented in Section 9.7 can be said to "proximate" the CDLIS environment. The analysis of Section 9.8 shows that the required error rates can be approximately met with a two-print system.

Requirement 5. The recognition process must be accomplished within 72 hours after receipt of the inquiry, and the verification processes must be accomplished within 5 seconds of receipt of the inquiry.

The recognition process throughput requirement can be met using equipment with the single comparison match rates calculated in Section 9.8. The verification process can be accomplished within 5 seconds.

Requirement 6. ...be capable of searching and comparing the 8.5 million current records and the 500,000 new CDL's issued each year... be capable of annually verifying the biometric records on 2 million CDL renewal applicants, 250,000 interstate residency change applicants and 90,000 applicants seeking duplicate licenses and the anticipated 6% a year growth in these types of applications.

[73] Ibid, page IV-D-9

[74] Ibid, page IV-D-12

The equipment throughput needed to meet this requirement was calculated in Section 9.8 and is believed to be within current vendor capabilities.

Requirement 7. The system must have a method of reporting management information.

All current AFIS have extensive management reporting capability.

Requirement 8: Deleted

Requirement 9. The system must be reliable.

Current AFIS installations, such as L.A. AFIRM or the State of New York Department of Social Services system have proven extremely reliable.

Requirement 10 ... on-site, immediate identification of whether or not an acceptable biometric sample has been obtained.

All current AFIS systems contain front-end quality control software, as described in Section 7.4.4 of this report, meeting Requirement 10.

Requirement 11. The system must be simple to use.

With regard to electronic fingerprinting in the Orkand study, to the statement "It is too hard to do?", only 5% of the 9,709 survey respondents answered 1 or 2 on a scale of 1(very) to 5 (not at all). Requirement 11 is met by all current AFIS.

Requirement 12. ...flexibility in procurement options

Internationally, there are at least six vendors with independent AFIS hardware/software systems available for applications on this scale. Further, there are at least another half dozen "system houses," who team rather fluidly with the primary vendors to supply large-scale systems. Any major Request for Proposal by a government agency can expect six to twelve serious responses from the AFIS industry.

Requirement 13. ... not require routine human intervention

Most current AFIS systems require no human intervention, although this must be carefully specified in the Request for Proposal as some vendors used to forensic systems still require human checking of pattern classification or feature extraction on the more difficult prints.

Requirement 14. ANSI/NIST fingerprint data format standards.

This report recommends that AAMVA adopt without change the ANSI/NIST "Data Format for the Interchange of Fingerprint Information," given as Appendix I, for all fingerprint data exchange.

Requirements 15 and 16: Deleted

15.0 STANDARDS DEVELOPMENT

Regardless of the final system architecture used, the CDL biometric system will require nationwide standards. Four standards are required and a fifth would be helpful:

1) a standard biometric identifier;
2) an image quality standard;
3) a data compression standard;
4) a data format standard;
5) a feature set standard.

Any non-commercial driver biometric identification system will require these standards as well. The existing NIST/ANSI/FBI standards in these areas are helpful points of departure, but were developed primarily for forensic applications. The FBI, in particular, does not develop standards for non-forensic applications. AAMVA, on the other hand, regularly develops "best practices" for the motor vehicle community. We are recommending that AAMVA take the lead in the development of biometric identification standards, as "best practices," in the first four areas in the application to driver's licensing.

15.1 A Standard Biometric Identifier

For reasons already discussed, we are recommending that fingerprints be adopted as the standard biometric identifier. However, a decision must be made as to which and how many prints to use. The advantages, with regard to both search time and false match error rate, of a multi-print system have been discussed. Rough calculations, showing that a two-print system would provide both adequate speed and false match accuracy, will be presented in the section on competing architectures. It will be our recommendation that two prints be used, but which two prints: thumbs or index fingers? Further, what will be the order of replacement, if those fingers are missing?

Social service systems now being commissioned are using forefingers for three primary reasons: forefingers are ergonomically easier to extend onto the platen, their core is closer to the end making it easier to center the core in the image, and they are thought not to carry the stigma of forensic fingerprinting and implied criminality to the extent thumbs do. Thumb prints have long been used for legal documents and in driver's licensing systems. Their primary advantage is that they are the least likely digit to be amputated or missing.

As determined by the AAMVA jurisdiction fingerprint survey, there is no standard finger for any system. The State of Texas, for instance, uses two thumb prints for drivers, two forefingers for social service recipients, and rolled ten-prints for criminals, child care workers and state employees. We believe that the choice of thumbs or forefingers, and replacement precedence, should be made by AAMVA, based on the impact of the choice on currently operating state systems.

15.2 Image Quality Standard

As mentioned elsewhere in this report, the FBI currently has an IAFIS Image Quality Specification for Scanners known as CJIS-RV-0010, Appendix G. "High end" image scanners (read "expensive") comply with this standard, which may be stricter than is needed for driver identification. Included in this report as Appendix H is a "strawman" scanner quality specification which may be more appropriate for non-forensic scanners. AAMVA should standardize the image quality requirements for non-forensic scanners as a "best practice," using Appendix H as an initial basis for development.

15.3 Data Compression Standard

ANSI, NIST and the FBI have developed the Wavelet Scalar Quantization Standard for fingerprint image compression, given as Appendix J of this report. We suggest that AAMVA adopt this standard. We recommend that a 20-to-1 compression ratio be adopted pending additional research on the effect of compression on error rates.

15.4 Data Format Standard

We recommend that AAMVA adopt without change the ANSI/NIST "Data Format for the Interchange of Fingerprint Information," given as Appendix I of this report, for all fingerprint data exchange.

15.5 Feature Set Standard

The development of standard features for fingerprint comparison is a controversial and difficult subject. NIST has held some preliminary discussions on this subject. Standards are absolutely required if there is to be any vendor independent storage of fingerprint information on driver's license documents. The vendor community largely opposes standards, however, because of the loss of perceived competitive advantage that would follow uniformity. Some government agencies oppose the development of feature standards precisely because this might allow for the exchange of fingerprints between non-related agencies. AAMVA should express to NIST interest in monitoring any standard development effort in this area, but we do not recommend that AAMVA attempt to independently enter this controversy.

16.0 BENEFIT-COST ANALYSIS

The primary goal of this section is to discuss issues related to a benefit-cost analysis of a biometric identification system that could be used as part of a driver's licensing system.

Theoretically, the benefits should exceed the cost for any system implemented. A common problem with determining the feasibility of a project is that benefits and/or costs are often hard to measure. Benefits and costs may be difficult to define precisely, or they may be intangible and difficult to convert into monetary terms.

With a system for identification related to commercial drivers' licenses, the benefits will principally be the net improvement in road safety resulting from removing, from the roads, commercial drivers whose licenses have been revoked or who have been driving with counterfeit, or other types of fraudulent licenses, and/or multiple licenses. In the case of collateral use of the system for purposes other than commercial driver identification, such as identification for social service applications, the total public benefit may be far broader. Such state applications, although reasonably expected given the current use of the driver's license as a general-purpose identification document, are beyond the scope of this study and benefit-cost analysis. It is appropriate to point out, however, that the true societal benefits may exceed those discussed in this limited study.

For the purpose of the discussion in this document, it will be assumed that the system will only be used for commercial drivers. Where appropriate, however, reference will be made to some of the possible implications if the system were to be used for other purposes.

Several options for the use and design of a biometric identification system have been discussed in this report. It is not possible to conduct a detailed benefit-cost analysis until the options are narrowed by policy decisions more carefully defining the purpose and scope of the system. It is possible, however, to perform a general analysis to determine what increased levels of road safety might be required, as a function of system cost, for benefit/cost justification.

The "cost" of the system will be considered as the dollar expense of the new system minus the dollar expense of any existing activities that the new system will replace. Included in the dollar expense of the new system are the costs of planning, designing, implementing, operating and maintaining the system. The "benefits" considered here will be limited to the savings in human life attributable to the implementation of the system. Creating a "benefit/cost" ratio requires both values to be measured in common units. Consequently, we will attempt to attach an arbitrary conversion value to the human life savings. A system that results in a dimensionless "benefit/cost" greater than one can be considered as justifiable.

It is also useful to create, in broad terms, a methodology for carrying out a benefit-cost analysis, should the decision be made to add a biometric identifier to the current commercial drivers' licensing system. Specifically, the following issues will be discussed in the remainder of the report:

- Some pertinent issues related to the benefit-cost analysis;
- The system benefit elements;
- The system cost elements;
- Some estimates of benefits and costs.

16.1 Some Pertinent Issues Related to the Benefit-Cost Analysis

There are a number of Federal Government initiatives related to benefit-cost analysis. These initiatives determine whether a project, in which the Federal Government has or potentially will have involvement, requires a benefit-cost analysis. In some cases, guidelines are provided for the analysis. The purpose of this section is to discuss some relevant Federal Government initiatives and documents as well as some issues emanating from them.

Four major Federal initiatives or documents will be addressed:

- Performance of commercial activities.
- Guidelines and discount rates for benefit-cost analysis of Federal programs.
- Principles for Federal infrastructure investments.
- Life cycle cost analysis.

16.1.1 Performance of Commercial Activities

Federal policy regarding the performance of commercial activities is stipulated in Circular No. A-76 by the Executive Office of the President, Office of Management and Budget (OMB) (1). The Circular was issued on August 4, 1983.

According to the Circular, the "Government shall not start or carry on any activity to provide a commercial product or service if the product or service can be procured more economically from a commercial source."

It has been the assumption of this report that the biometric system and system integration functions would be provided by the private sector. In fact, this may be a requirement under Circular No. A-76.

16.1.2 Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs

Some guidelines regarding benefit-cost, cost-effectiveness and lease purchase analysis were issued by the Executive Office of the President, OMB, on October 29, 1992, in Circular A-94 (2). A copy of the Circular is provided in Appendix M. These guidelines are to be used by agencies evaluating Federal activities and must be followed in all analyses submitted to OMB in support of legislative and budget programs.

According to the Circular, the guidelines "apply to any analyses to support Government decisions to initiate, renew, or expand programs or projects which would result in a series of measurable benefits or costs extending for three or more years into the future." One of the activities that are specifically exempted from the scope of the Circular, is the acquisition of commercial-type services by government or contractor operation for which guidance is provided in Circular No. A-76 (discussed in the previous section). Since the implementation of a biometric identification system would result in benefits and costs extending for more than three years into the future, the system ought to be subjected to a formal benefit-cost analysis when the scope and function of the project have been more fully defined.

In addition to defining terms, the following issues are specifically addressed in the document:

- General principles of cost-benefit and cost-effectiveness analysis.
- Identifying and measuring benefits and costs.
- Treatment of inflation.
- Discount rate policy.
- Treatment of uncertainty.
- Incidence and distributional effects.
- Special guidance for public investment analysis.
- Special guidance for regulatory impact analysis.
- Special guidance for lease-purchase analysis.
- Related guidance.

A brief discussion of some of the salient points, presented in the Circular, follows.

a) The policy rationale for the program should be clearly stated in the analysis.

This is an important issue for the biometric identification system under consideration. This report discusses possible functions and designs for such a system, but the policy rationale is beyond the scope of this study. In fact, as pointed out in Section 2.0 of this report, Section 9105 of the Truck and Bus Safety and Regulatory Reform Act does not make clear the policy rationale for this program. Any movement toward the implementation of this system may require the development by FHWA of a comprehensive rationale.

Section 9105 of the Truck and Bus Safety and Regulatory Reform Act extends only to commercial drivers, any initial system would only cover commercial drivers. However, stating that a system is or would be designed for commercial drivers is by itself not adequate and deserves further scrutiny. At least three different systems, with three different rationales, could be designed by states to meet this purpose:

1. A system solely designed for commercial drivers' licensing.
2. A system that would accommodate commercial drivers' licensing as part of a larger system, which would serve more than commercial drivers.

3. A system that would initially only include commercial drivers and that could readily be expanded to meet other objectives.

Serving only commercial drivers, the benefits for all three systems will be the same, but the systems could have different costs. For instance, in the case of the second and third systems, the benefit/cost ratios for the commercial driver portion of the system may be lower than the benefit/cost ratio for the first system.

b) Evaluation of alternatives.

The evaluation of alternatives should involve considering alternative means to achieve the program objectives, by "examining different program scales, different methods of provision and different degrees of government involvement." This could, of course, lead to several alternatives for a program of this sort.

The issue of different degrees of government involvement is in this case very pertinent. Since several states and various organizations within each state may be involved, it may be quite complicated to determine the degree of government involvement. Also, because the implementation may involve several government and private organizations, the cooperation of many or all the states will be required.

c) Retrospective studies.

Retrospective studies to determine whether the anticipated benefits and costs have been realized should be considered. In view of the lack of comprehensive data regarding the current scope of the problem, the benefits to be accrued, and the costs of the biometric identification system, a program of monitoring the benefits and costs should be considered.

d) Identifying and measuring benefits and costs.

It is stated that social net benefits and costs should be measured, and not the benefits and costs to the Federal Government. This point is often misunderstood and explains the impetus of this section of our report to take up considerations outside of the commercial driver's licensing boundaries.

e) Discount rate.

A real discount rate of seven percent is recommended, but other discount rates should be used as part of a sensitivity analysis.

f) Sensitivity analysis.

Sensitivity analysis should be considered for estimates of the discount rate, benefits and costs, the general inflation rate and distributional assumptions.

g) Analysis of excess burdens.

A supplementary analysis, wherein costs should be multiplied by a factor of 1.25, for public investments that are not justified on the basis of cost savings, should be presented. This requirement applies to public investments with social benefits apart from decreased Federal costs. Since the benefits of this project will primarily consist of social benefits, a supplementary analysis should be performed.

16.1.3 Principles for Federal Infrastructure Investments

In Executive Order 12893 titled "Principles For Federal Infrastructure Investments," issued by the Office of the Press Secretary of the White House on January 27, 1994 (3), it is stated that Federal spending for infrastructure programs shall include spending and grants for transportation. The principles of Federal infrastructure investment are discussed under the following major headings:

- Systematic analysis of expected benefits and costs.
- Efficient management.
- Private sector participation.
- Encouragement of more effective state and local programs.

The Order refers to some of the same issues outlined in OMB Circular A-94 and it is required in the Order that the analytical methods outlined in the Circular be followed when implementing the investment principles. A copy of the order is provided in Appendix N.

Although the system under consideration in this project is not what is usually thought of as transportation infrastructure, expenditure for the system may be subject to the procedures outlined in the order, because it is a major project falling under the jurisdiction of the FHWA. This issue could be clarified by the FHWA, but the requirements, outlined in OMB Circular A-94 (2), appear to require that this project be subjected to these principles.

16.1.4 Life-Cycle Cost Analysis

A final policy statement regarding life-cycle cost analysis for the FHWA was published in the Federal Register Vol. 61, No. 182 on September 18, 1996 (4). A copy of the Order is provided in Appendix O. The policy helps to fulfill the requirements set forth in Executive Order 12893 (3), discussed above.

The policy is directed towards the application of life-cycle costs related to highways and related infrastructure investments. It will be up to the FHWA to determine whether the biometric identification system is included as a "related infrastructure investment." Again, this may be redundant if the system should undergo benefit-cost analysis as required in the OMB Circular A-94 (2).

16.1.5 Some Conclusions and Recommendations

From the review of the Federal initiatives and documents, it appears that there is an increasing emphasis on benefit-cost analysis. According to the guidelines for benefit-cost analysis contained in Circular No. A-94 (2), issued by the Executive Office of the President, Office of Management and Budget, on October 29, 1992, it appears a biometric identification system should be subjected to a formal benefit-cost analysis when the full scope and function of the system has been determined.

16.2 Benefits

As stated before, the benefits will principally be the saving in accident costs resulting from the implementation of the biometric identification system. The success of the system in doing so will depend on each of the system components and specifically the probability that the each will perform its function.

We have put together a first-order, highly simplified mathematical model for the calculation of the benefits accrued through a decrease in accidents. This model will serve to clarify the parameters for which hard data will be needed for formal calculation of the benefit/cost ratio. A more advanced model will require these same parameters.

Total number of accidents saved per year = $ACC_{rem} + ACC_{det}$

where:

ACC_{rem} = number of accidents saved per year as a result of drivers not going back to driving after being jailed or having their licenses revoked

ACC_{det} = number of accidents saved per year as a result of drivers deterred from driving as a result of the implementation of a biometric system

ACC_{rem} for each system alternative can be determined as follows:

$ACC_{rem} = D_j * P_a * P_n$

D_j = number of offending drivers who are detected and then convicted

P_n = the proportion of the year that offending drivers who are convicted do not drive commercial vehicles (may be greater than 100%)

P_a = proportion of offending drivers who get involved in an accident on an annual basis.

We can further write

$P_a = N_o/D_o$

where

N_o= the number of annual accidents involving offending drivers

D_o = the number of offending drivers on the road.

Further:

$D_j = D_c*P_s*P_o*P_d*P_j$

where

D_c = number of commercial drivers in the driver pool

P_s = proportion of commercial drivers screened

P_o = proportion of screened drivers who are offending

P_d = proportion of offending drivers who are detected by the biometric system

P_j = proportion of detected drivers that are convicted

P_d, the portion of the offending drivers who are detected, is directly impacted by the error rates of the biometric system. A more precise calculation of P_d from the system error rates is dependent upon the system function and decision policy, as discussed in Appendix F.

Finally:

ACC_{rem} = number of accidents saved on an annual basis by removing offending drivers $= D_c*P_s* P_o*P_d*P_j*P_n* N_o/D_o$

This relationship indicates the data that will be needed to estimate the number of accidents saved directly by removing offending drivers from the road. Estimating the accidents saved by deterrence may be impossible or, at best, very difficult. Some of the values required for both relationships could be estimated from historical data, others determined by policy or theory. Some can only be based on tests carried out on newly designed systems.

The following numbers and proportions could be estimated from historical data:

D_c = number of commercial drivers in the driver pool.
P_o = proportion of screened drivers who are offending.
P_j = proportion of detected drivers who are convicted.

P_n = the proportion of the year that an offending driver who is convicted does not drive commercial vehicles.

N_o= the number of accidents per year involving offending drivers.

The proportion of commercial drivers screened, P_s, could be controlled by system policy. The proportion of offending drivers who are detected by the biometric system, P_d, will depend upon the system error rates and can be estimated when the system is more fully specified. As previously discussed, determining D_o , the number of offending drivers on the road, has been the focus of the CDLIS effectiveness studies. Consequently, determining the benefit of a biometric commercial driver identification system cannot proceed without a valid approximation of the number of offending drivers.

An estimate of the initial and annual reduction in accident costs, resulting from the implementation of the biometric identification system, could be obtained by multiplying the total number of accidents saved by the value of each accident.

16.3 Some Estimates of Benefits

In CDLIS Effectiveness Study carried out by the Department of Motor Vehicles in New York (5), it was shown that the CDLIS system probably deters drivers from obtaining multiple licenses. No evidence was found that drivers with multiple licenses exist. Under these circumstances, there will be no benefits derived from having a biometric system that deters drivers from obtaining multiple licenses. A system, which will aid in removing from the roads drivers with fraudulent licenses, including multiple drivers with single licenses, could have benefits.

As discussed above, it is impossible at this time to carry out a complete benefit-cost analysis, since the system has not yet been specified and the number of drivers with duplicate or fraudulant licenses is not known. Some idea could be formed, however, of the hypothetical value of different levels of accident savings and, consequently, the corresponding amount that could be spent on a biometric identification system.

Some idea of the potential benefit in dollar amounts can be obtained by looking at some accident costs. The National Safety Council (NSC) has provided values for comprehensive accident costs (6). These values are shown below in 1994 dollars, as provided and adjusted to 1996, using the implicit price deflator for the gross domestic product, as estimated by the Department of Commerce, Bureau of Economic Analysis. The values are on a per person basis.

Table 1: Value of a Single Accident by Type

Type of Accident	1994 value	1996 value
Death	$2,890,000	$3,022,200
Incapacitating injury	$193,000	$201,800
Non-incapacitating evident injury	$44,000	$46,000
Possible injury	$23,000	$24,100
No injury	$2,600	$2,700

The annual worth as well as the present worth of different numbers of fatalities are shown in the following table. In order to make these calculations, the following assumptions were made:

- Cost of a fatality: $3,022,200
- Useful life of the system: 10 years
- Real discount rate: 7%

It should be noted that a calculation of the present value of annual accident cost savings should ideally account for projected year-to-year-changes in accident rates. For the sake of simplicity, this was neglected.

Table 2: Value Of Fatalities Prevented

Number of fatalities prevented per year	Annual worth (millions of dollars)	Present worth (millions of dollars)
1	3.0	21.2
2	6.0	42.5
3	9.1	63.7
4	12.1	84.9
5	15.1	106.1
10	30.2	212.3
20	60.4	424.5
50	151.1	1,061.3
100	302.2	2,122.7

In Section 12 of this report, we implied that the total cost of the system, depending upon function and design, would be on the order of a couple of tens of millions of dollars. Table 2 implies that an initial investment $20 million for a biometric identification system (as guess-timated in Section 11.1) could be justified if just one life per year was saved over the ten year life-span of the system. Could the system reasonably be expected to save one life per year?

The magnitude of the problem of fraudulently licensed drivers can be understood by considering statistics for all drivers. According to the National Highway Traffic Safety Administration (NHTSA), 6,409 drivers with an invalid license were involved in fatal crashes out of a total of 54,016 drivers involved in fatal crashes in 1995 (7). This amounts to a proportion of 11.9 percent of all fatal crashes (all cars and trucks) involving drivers with invalid licenses. According to statistics provided by the FHWA, there were 4,849 fatalities, in 1993, which involved medium and heavy trucks out of a total of 40,115 fatalities, involving motor-vehicles (8). If we make an "upper bound" assumption that 11.9 percent of the fatalities involving medium and heavy trucks could have been avoided by preventing the drivers with invalid licenses from driving, then 577 fatalities could have been prevented. This would amount to an upper bound on savings in accident costs of 1.7 billion dollars (in 1996 dollars). Clearly, the existing systems make it far more difficult for commercial drivers than general drivers to operate with fraudulent licenses.

It should be noted that the numbers, presented in the previous paragraph, do not allow for some incompatibility between different years' statistics and some differences in definitions. For the purpose of the discussion presented here, the accuracy is considered adequate. Further, it is unlikely that all 577 accidents could have been prevented by preventing the unlicensed drivers from driving. Moreover, it is unlikely that the unlicensed drivers were at fault in all accidents and that a licensed driver could have prevented the accident from occurring. On the other hand, the savings in injury and non-injury accident costs will increase the value substantially.

The upper bound on accident costs of 1.7 billion dollars is significant and would justify the consideration of a biometric identification system, even if incorrect by two orders of magnitude.

16.4 Costs

The costs are comprised of the cost planning, designing, implementing, operating and maintaining the system. These costs include both equipment cost and the cost of activities, necessary to support the above processes. Also, activities which will be replaced by any of the above activities, should be identified and the cost thereof subtracted from the cost of the new system.

In order to determine the cost, the system will have to be specified to the extent that the individual components can be priced. The specification will differ depending upon the function of the system, as outlined in Section 4, and the central vs. decentralized design issues, as discussed in Section 11. Any careful estimation of cost will have to await policy decisions regarding the scope and function of the system. For guess-timation purposes, a cost of $20M can be used for the identification part of the system, excluding a roadside verification capability.

16.5 References for Benefit-Cost Study

1. *Performance of Commercial Activities.* Circular No. A-76. Executive Office of the President, Office of Management and Budget, August 4, 1983.

2. *Guidelines And Discount Rates For Benefit-Cost Analysis Of Federal Programs.* Circular No. A-94. Executive Office of the President, Office of Management and Budget, October 29, 1992.

3. *Principles For Federal Infrastructure Investments.* Executive Order 12893. Office of the Press Secretary, The White House, January 27, 1994.

4. *Life Cycle Cost Analysis. Federal Highway Administration Docket No. 94-15.* Federal Register Vol. 61, No. 182, September 18, 1996.

5. New York State CDLIS Effectiveness Study, 1997
6. *Accident Facts, 1995 Edition.* National Safety Council, Itasca, Illinois, 1995.
7. *Traffic Safety Facts 1995.* National Highway Traffic Safety Administration, Washington D.C., 1996.
8. *Our Nation's Highways. Selected Facts and Figures.* Federal Highway Administration, Washington D.C., 1995.

17.0 Conclusions

This study recommends that fingerprinting be established as the biometric for identifying drivers pursuant to Section 9105 of the "Truck and Bus Safety and Regulatory Reform Act", Public Law 100-690 This study further defines the minimum required scope of the system and recommends specific "minimum uniform standards" for the biometric identification of commercial drivers using fingerprinting. We have included results of a recent large-scale fingerprinting test showing the feasibility of two-finger systems at a scale comparable to the current CDLIS enrollment.

We suggest several standards (scanner image quality, compression, data transmission format) for adoption by AAMVA as "best practices" and outline several system approaches for using biometric fingerprint technology to enforce the "one-driver, one-license, one-record" mandate of the Commercial Motor Vehicle Safety Act. In the absence of hard information supporting the existence of a problem with multiple licenses or single licenses with multiple drivers, we have difficulty in computing the benefit-cost feasibility of such a system, but have included a computational methodology for use as such data becomes available.

We recommend that the FHWA cooperate with AAMVA to establish "Best Practices" for biometric identification using the fingerprint, including standards for finger selection, scanner image quality, compression technique and data transmission format, based on the specific recommendations of this report in these areas. We further recommend that AAMVA create model fingerprint collection and protection legislation to serve as a guide for states wishing to begin the fingerprint identification of commercial drivers.